INGENIERÍA SOCIAL

EL ARTE DEL HACKING PERSONAL

Christopher Hadnagy
Prólogo de Paul Wilson





Christopher Hadnagy

Christopher Hadnagy es el desarrollador principal de *www.social-engineer.org,* el primer marco teórico de ingeniería social del mundo. En más de 14 años de actividad profesional en los campos de la seguridad y las tecnologías de la información, ha estado asociado al equipo de www.backtrack-linux.org y trabajado en una gran variedad de proyectos de seguridad. También ejerce como preparador e ingeniero social principal en el equipo de pruebas de seguridad de Offensiv.



Ingeniería social
El arte del hacking personal

Christopher Hadnagy



TECNOLOGÍA MULTIMEDIA

TÍTULO DE LA OBRA ORIGINAL:
Social Engineering. The Art of Human Hacking

RESPONSABLE EDITORIAL:
Eugenio Tuya Feijoó
Lorena Ortiz Hernández

TRADUCTOR:
Álvaro Montero Marín

DISEÑO DE CUBIERTA:
Cecilia Poza Melero

Ingeniería social
El arte del hacking personal

Christopher Hadnagy



Edición española:

© EDICIONES ANAYA MULTIMEDIA (GRUPO ANAYA, S.A.), 2011
Juan Ignacio Luca de Tena, 15. 28027 Madrid
Depósito legal: M. 22.475-2011
ISBN: 978-84-415-2965-6
Printed in Spain
Impreso en: Fernández Ciudad, S. L.

A mi preciosa mujer y mi maravillosa familia;
sin vosotros esto no hubiera sido posible.
Mati, no hay palabras para expresar la gratitud
que siento por lo que has hecho.

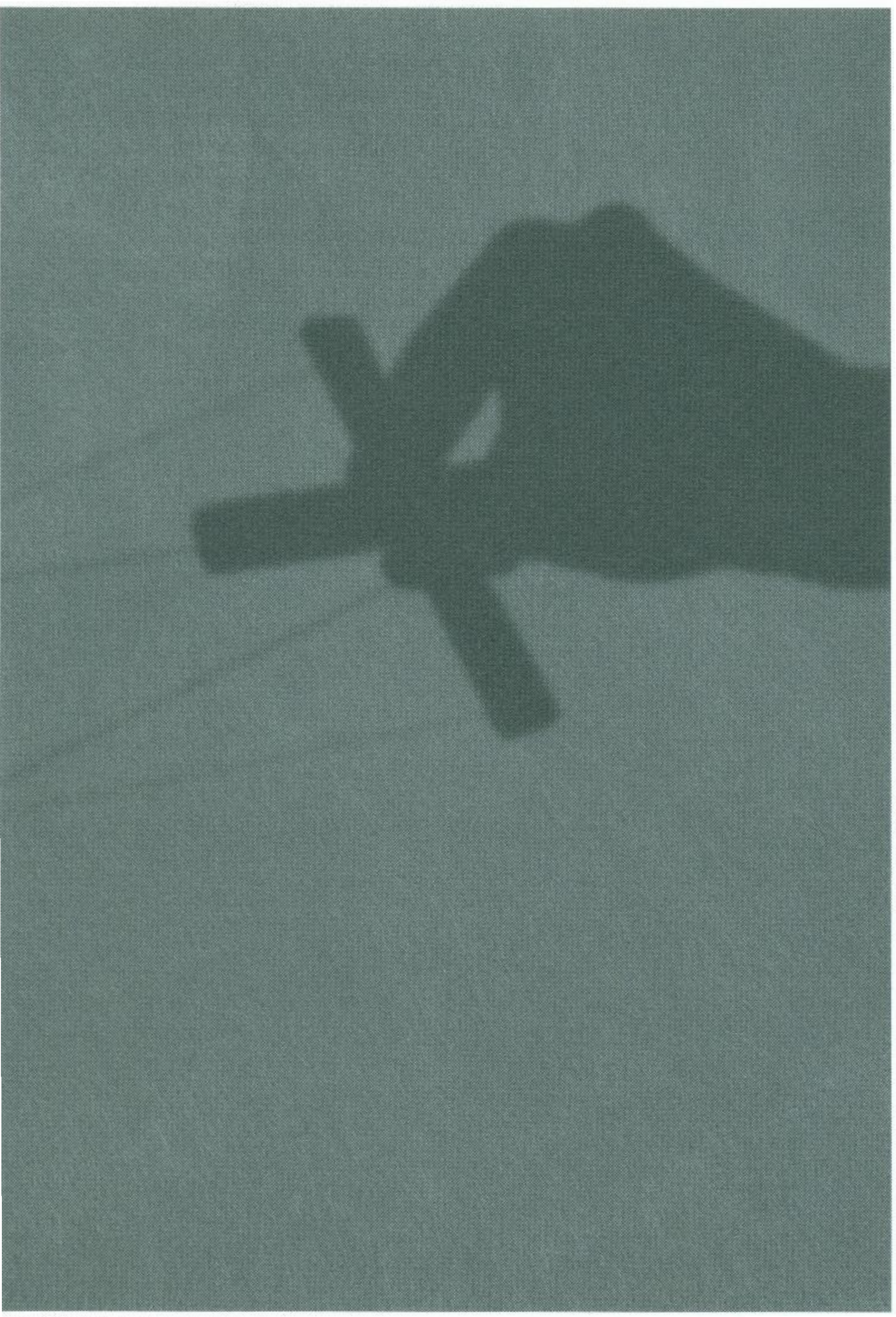
Sobre el autor

Christopher Hadnagy es el desarrollador principal de www.social-engineer.org, el primer entorno de ingeniería social del mundo. En más de 14 años de actividad en seguridad e IT, ha estado asociado al equipo de www.backtrack-linux.org y ha trabajado en una gran variedad de proyectos de seguridad. También ejerce como preparador e ingeniero social principal en el equipo de pruebas de seguridad de Offensive Security.

Sobre el editor técnico

Jim O'Gorman es *cracker* profesional y auditor de ingeniería social con más de 14 años de experiencia trabajando para empresas que van desde pequeños proveedores de servicios de Internet (ISP, *Internet Service Provider*), a grandes corporaciones de la lista Fortune 100. Jim es copreparador de la clase avanzada de Offensive Security de explotación de Windows, una de las clases de desarrollo de explotación más difíciles. Miembro fundador de www.social-engineer.org, Jim es una autoridad educando sobre las amenazas de la ingeniería social.

Índice



Prólogo

La seguridad es una moneda de dos caras: por un lado, buscamos un sentido de comodidad y seguridad; por el otro, ladrones, hackers y vándalos buscan resquicios. La mayoría de nosotros creemos que nuestras casas son seguras hasta que un día nos encontramos fuera, sin poder entrar. De pronto, nuestra perspectiva cambia y encontramos las debilidades fácilmente.

Para entender por completo cualquier tipo de seguridad, es fundamental "saltar la valla" para, en esencia, "encerrarnos" fuera y empezar a buscar otras formas de entrar.

El problema es que la mayoría de nosotros no vemos los problemas potenciales porque estamos cegados por nuestra propia confianza o por nuestra creencia de que unos cerrojos fuertes, unas puertas gruesas, un sofisticado sistema de seguridad y un perro guardián son más que suficientes para mantener a la mayoría de la gente a raya.

Yo no soy como la mayoría de la gente. En los últimos diez años, he llevado a cabo más timos y estafas que nadie en la historia. He vencido a casinos, he amañado eventos deportivos y subastas, he convencido a gente para desprenderse de sus posesiones más queridas y he pasado caminando por delante de niveles de seguridad aparentemente imbatibles.

Me he ganado la vida poniendo al descubierto los métodos de ladrones, embaucadores, pillos y timadores en un exitoso programa de televisión llamado *The Real Hustle*. Si hubiera sido un verdadero criminal, probablemente sería rico, famoso o estaría muerto (o puede que las tres cosas). He utilizado toda una vida de investigación de todas las formas de engaño para enseñarle al público lo vulnerable que es en realidad.

Todas las semanas, junto a Alexis Conran, llevo a cabo timos a gente real que no tiene ni idea de que está siendo estafada. Utilizando cámaras ocultas, mostramos a la audiencia en sus casas los posibles timos para que puedan reconocerlos.

Esta carrera atípica ha dado como resultado un entendimiento único sobre cómo piensan los criminales. Me he convertido en un cordero con piel de lobo. He aprendido que no importa que algo pueda parecer imposible, casi siempre hay una forma ingeniosa e inesperada de resolver el problema.

Un ejemplo es cuando me ofrecí para mostrar lo sencillo que es no sólo robarle el bolso a una mujer, sino también conseguir que me diga la clave de sus tarjetas de crédito. La BBC no creía que esto pudiera lograrse. Cuando presentamos esta idea para el programa, el jefe de la BBC escribió al lado "esto nunca sucederá" y envió el proyecto de vuelta. Sabíamos que era perfectamente posible porque se habían denunciado diferentes versiones de un mismo timo en el que las víctimas eran persuadidas para revelar sus claves secretas en ingeniosas estafas por todo el Reino Unido.

Tomamos elementos de distintos timos para poder ilustrar exactamente cómo alguien podría ser engañado para darle a otra persona acceso completo a su cuenta bancaria.

Para hacer la demostración preparamos el timo en una cafetería que estaba en la planta superior de un centro comercial de la calle Oxford, en Londres. La cafetería estaba muy tranquila cuando entré vestido con traje y corbata y me senté en una mesa libre. Coloqué mi maletín sobre la mesa y esperé la víctima adecuada. Momentos después, llegó la víctima con un amigo y se sentó en una mesa junto a la mía, dejando su bolso en una silla junto a ella. Acercó la silla y mantuvo la mano sobre el bolso en todo momento, como era probablemente su costumbre.

Tenía que robar el bolso, pero con su mano apoyada sobre él y su amigo sentado enfrente, parecía que iba a ser muy complicado. No obstante, unos minutos después, su amigo se levantó para ir al servicio. La víctima estaba sola, así que hice la señal a Alex y Jess.

Haciendo el papel de una pareja, Alex y Jess le pidieron a la víctima si podía hacerles una foto juntos. Ella se ofreció amablemente a hacerla. Quitó la mano del bolso para coger la cámara y hacer la foto de la "pareja feliz" y, mientras estaba distraída, alargué la mano disimuladamente, cogí el bolso y, con calma, lo metí

dentro de mi maletín. Cuando Alex y Jess se fueron de la cafetería la víctima todavía no había reparado en la silla vacía. Cuando ya no estaban al alcance de su vista, Alex se dirigió rápidamente al aparcamiento.

La víctima no tardó mucho en darse cuenta de que su bolso había desaparecido. Le entró el pánico al instante. Se levantó y buscó a su alrededor desesperada. Esto era exactamente lo que buscábamos, así que le pregunté si necesitaba ayuda.

Me preguntó si había visto algo. Le dije que no, pero la convencí para que se sentara y pensara lo que había en el bolso. Un teléfono móvil. Maquillaje. Algo de dinero. Y su tarjeta de crédito. ¡Bingo!

Le pregunté cuál era su banco y después le dije que yo trabajaba en ese banco. ¡Menudo golpe de suerte! La tranquilicé diciéndole que todo iría bien pero le dije que tenía que cancelar su tarjeta de crédito inmediatamente. Llamé al teléfono de ayuda del banco, que en realidad era Alex y le pasé mi teléfono a ella. Ya había picado el anzuelo, ahora Alex sólo tenía que recoger el carrete.

Alex estaba abajo en la furgoneta. Sobre el salpicadero había un reproductor de CD en el que sonaban ruidos de oficina que habíamos bajado de Internet. Mantuvo tranquila a la víctima, le dio falsas esperanzas y después le aseguró que su tarjeta podía cancelarse fácilmente pero, para verificar su identidad, debía introducir la clave secreta tecleándola en el teléfono móvil.

Mi teléfono móvil.

Puede imaginar el resto. Una vez que tuve su clave secreta, salí de la cafetería. Si hubiéramos sido ladrones de verdad, tendríamos acceso a su cuenta bancaria a través de retiradas de dinero en cajeros automáticos y compras con chip y clave secreta. Por suerte para ella, sólo era un programa de televisión y se puso muy contenta cuando regresé para devolverle el bolso y decirle que todo había sido un timo falso. Incluso me dio las gracias por devolverle el bolso, a lo que le respondí: "No me des las gracias. Fui yo quien te lo robó".

No importa lo seguro que sea un sistema, siempre hay un modo de penetrar en él. A menudo, los elementos humanos del sistema son los más fáciles de manipular y engañar. Crear situaciones de pánico, ejercer influencias o tácticas de manipulación o provocar sentimientos de confianza son métodos para hacer que la víctima se relaje.

El escenario mostrado aquí es un ejemplo extremo, pero pone en evidencia que, con un poco de creatividad, timos en apariencia irrealizables pueden llevarse a cabo.

El primer paso para aumentar la seguridad es simplemente admitir que un sistema es vulnerable y puede ponerse en peligro. Por el contrario, creer que es imposible que haya una brecha nos pone una venda sobre los ojos mientras avanzamos a toda velocidad. Este libro está diseñado para ofrecerle una valiosa comprensión de los métodos utilizados para romper sistemas aparentemente

seguros y poner al descubierto las amenazas que existen sobre lo más vulnerable, las personas. Este libro no es una guía para hackers, ellos ya saben cómo penetrar y encuentran nuevas formas cada día. En lugar de eso, Chris Hadnagy ofrece a aquéllos que se encuentran dentro de la valla la oportunidad de echar un vistazo desde el otro lado, el lado oscuro, mientras pone al descubierto la forma de pensar y los métodos de los hackers más maliciosos del mundo, timadores e ingenieros sociales.

Recuerde que quienes construyen vallas piensan diferente de quienes tratan de cruzarlas, rodearlas, pasarlas por debajo o atravesarlas. Como suelo decirle a mis audiencias, si cree que a usted no le pueden timar, es justo la persona que me gustaría conocer.

Paul Wilson
Octubre de 2010



Prefacio y agradecimientos

Fue hace pocos años cuando estaba sentado con mi amigo y mentor Mati Aharoni decidiendo el lanzamiento de `www.social-engineer.org`. La idea fue creciendo y creciendo hasta convertirse en un espectacular sitio Web mantenido por gente realmente brillante. Poco después, se me ocurrió plasmar todos esos años de investigación y experiencia en las páginas de este libro. Cuando tuve la idea, encontré un apoyo impresionante. Dicho esto, es necesario hacer alguna mención especial para entender cómo este libro se convirtió en lo que hoy es.

Desde una edad muy temprana, siempre estuve interesado en manipular a la gente. No en el mal sentido, pero me parecía interesante la cantidad de veces que era capaz de conseguir cosas o verme en situaciones que parecían impensables. En una ocasión, estaba con un buen amigo y socio empresarial en una conferencia técnica en el Javits Center de Nueva York. Una gran corporación había alquilado la famosa juguetería FAO Schwarz para una fiesta privada. Por supuesto, para entrar en la fiesta hacía falta invitación, mi amigo y yo éramos dos peces pequeños en un gran estanque: la fiesta era para los directivos de empresas como HP, Microsoft y otras del estilo. Mi amigo me dijo: "Estaría muy bien poder ir a esa fiesta".

Yo simplemente respondí: "¿Y por qué no hacerlo?". En ese momento pensé: "Estoy seguro de que podemos entrar si lo pedimos de la forma correcta". Así que me acerqué a las mujeres de la taquilla encargadas de la lista de invitados y hablé

con ellas durante unos minutos. Entonces, apareció Linus Torvalds, el creador de Linux. Yo había cogido un muñeco de peluche de Microsoft de un *stand* y en plan de broma le dije a Linus: "Oye, ¿puedes firmarme un autógrafo en el muñeco de Microsoft?".

Linus se rió mucho con la broma y, mientras sacaba sus invitaciones, dijo: "Buen golpe, chaval, nos vemos en la fiesta".

Cuando me volví hacia las mujeres de la taquilla, me dieron dos invitaciones para la exclusiva fiesta en FAO Schwarz.

No fue hasta más adelante cuando empecé a analizar historias como ésta, después de que algunos empezaran a llamarlo "el efecto Hadnagy". Aunque sonaba divertido, empecé a darme cuenta de que muchas de las cosas que me habían ocurrido no tenían que ver con la suerte o el destino, sino más bien con saber dónde estar en el momento oportuno.

Esto no significa que no haya sido necesario mucho trabajo y mucha ayuda por el camino. Mi musa en la vida es mi maravillosa mujer. Durante casi dos décadas me has apoyado en todas mis ideas y esfuerzos y eres mi mejor amiga, mi confidente y mi pilar de apoyo. Sin ti no estaría donde estoy. Además, has engendrado a dos de los niños más bonitos de este planeta. Mi hijo y mi hija son la motivación para seguir haciendo todo esto. Si algo de lo que hago puede hacer de éste un lugar más seguro para ellos o enseñarles cómo mantenerse a salvo, entonces todo habrá merecido la pena.

Para mis hijos, no puedo expresar suficiente gratitud por vuestro apoyo, amor y motivación. Tengo la esperanza de que mi hijo y mi pequeña princesa no tengan que tratar con las malas personas de este mundo, pero soy consciente de lo improbable que es esto. Que esta información os mantenga a los dos un poco más seguros.

Paul, alias *rAWjAW*, gracias por toda tu ayuda con el sitio Web. Las miles de horas que pasaste como "wiki-master" han dado resultado y ahora tenemos un estupendo recurso que puede ser utilizado por todo el mundo. Ya sé que no lo digo lo suficiente pero: "¡Estás despedido!". En combinación con la preciosa creación de Tom, alias *DigIp*, el sitio Web es una obra de arte.

Carol, mi editora en Wiley, se ha dejado la piel para organizar todo esto y que siguiera algo parecido a una cronología. Ha hecho un trabajo increíble reuniendo un gran equipo humano y convirtiendo esta idea en una realidad. Gracias.

Brian, lo decía en serio. Voy a echarte de menos cuando esto se acabe. Después de trabajar contigo durante los últimos meses, empecé a esperar ansioso mis sesiones de edición y el conocimiento que me brindabas. Tus honestas recomendaciones y tus francos consejos han hecho este libro mejor de lo que era.

También transmito mi gratitud a Jim, alias *Elwood*. Sin ti muchas de las cosas que han sucedido en `social-engineer.org`, así como en este libro y, caray, en mi vida en los últimos dos años no serían una realidad. Gracias por mantenerme

humilde y bajo control. En todo momento has conseguido que mantuviese los pies en la tierra, ayudándome a permanecer concentrado y a equilibrar los distintos papeles que he tenido que jugar. Gracias.

Liz, hace unos doce años me dijiste que debía escribir un libro. Estoy seguro de que tenías algo diferente en mente, pero aquí está. Me has ayudado durante tiempos bastante oscuros. Gracias, te quiero.

Mati, mi mentor y mi *achoti*, ¿dónde estaría yo sin ti? Mati, de verdad eres mi mentor y mi hermano. Gracias de todo corazón por tener fe en que podía escribir este libro y lanzar `www.social-engineer.org` y en que ambas cosas fueran buenas. Más que eso, tu constante consejo y dirección se han trasladado a las páginas de este libro para hacer de mí mucho más de lo que pensaba que podía ser.

Tu apoyo con el equipo de BlackTrack, junto con el apoyo al equipo en `www.offensive-security.com`, ha trascendido todo lo que cabría esperar. Gracias por ayudarme a equilibrar y priorizar. Mi *achoti*, un agradecimiento especial para ti por ser la voz de la razón y la luz al final de algunos días frustrantes. Con todo mi cariño, te doy las gracias.

Todas las personas que he mencionado contribuyeron en este libro de uno u otro modo. Con su ayuda, apoyo y amor, este libro se ha convertido en un trabajo del que estoy orgulloso. Para el resto de vosotros que habéis colaborado con el sitio Web, el canal o nuestra investigación, gracias.

Al leer este libro, espero que le afecte de la misma manera que a mí me ha afectado escribirlo.

Albert Einstein dijo una vez: "La información no es conocimiento". Ése es un pensamiento poderoso. Una simple lectura de este libro no es suficiente para alcanzar este conocimiento. Aplique los principios, practique lo que se enseña en estas páginas y haga que la información forme parte de su día a día. Al hacerlo, verá que el conocimiento es realmente útil y poderoso.

Chistopher Hadnagy
Octubre de 2010



1. Una mirada al mundo de la ingeniería social

Si conoces a los demás y te conoces a ti mismo, ni en cien batallas correrás peligro.
Sun Tzu

La ingeniería social ha sido en gran parte incomprendida, lo que ha conducido a muchas opiniones diferentes sobre lo que es la ingeniería social y cómo funciona. Esto ha llevado a una situación en la que algunos pueden pensar que la ingeniería social es simplemente mentir para lograr insignificantes artículos gratis, como pizza, o para obtener satisfacción sexual; otros piensan que la ingeniería social se refiere exclusivamente a las herramientas utilizadas por los delincuentes o estafadores o, quizá, que se trata de una ciencia cuyas teorías pueden dividirse en partes o ecuaciones y ser estudiadas. O a lo mejor es un arte místico oculto que otorga a sus practicantes la habilidad para realizar poderosos trucos mentales, como un mago o un ilusionista.

Sea de la opinión que sea, este libro es para usted. Gente normal utiliza a diario la ingeniería social en situaciones normales. Una niña intentando abrirse paso en el pasillo de las golosinas o un empleado intentando lograr un aumento están utilizando la ingeniería social. La ingeniería social tiene lugar a nivel gubernamental

o en el marketing de un pequeño negocio. Por desgracia, también está presente cuando delincuentes, estafadores y personas por el estilo engañan a la gente para sonsacarles información que los hace vulnerables a un delito. Como cualquier herramienta, la ingeniería social no es ni buena ni mala, es simplemente una herramienta con muy diversos usos.

Para entender esta idea, considere estas cuestiones:

- ¿Le han encargado que su empresa sea lo más segura posible?
- ¿Es un entusiasta de la seguridad que lee toda la información nueva que va saliendo?
- ¿Es un auditor informático profesional contratado para evaluar la seguridad de sus clientes?
- ¿Es un estudiante universitario que ha elegido como asignatura algún tipo de especialización en tecnologías de la información?
- ¿Es actualmente un ingeniero social buscando nuevas ideas para poner en práctica en su trabajo?
- ¿Es un consumidor preocupado por los peligros del fraude y el robo de identidad?

Sea cual sea su situación, la información contenida en este libro le descubrirá cómo utilizar las habilidades de la ingeniería social. También curioseará en el lado oscuro de ésta y aprenderá cómo utilizan estas habilidades los "chicos malos" en beneficio propio. A partir de ahí, sabrá cómo ser menos vulnerable a los ataques de ingeniería social.

Una advertencia por adelantado: este libro no es para débiles. Le lleva a esos rincones oscuros de la sociedad donde viven los piratas informáticos, los maliciosos hackers. Descubre y ahonda en áreas de la ingeniería social utilizadas por espías y estafadores. Examina tácticas y herramientas que parecen sacadas de una película de James Bond. Además, aborda situaciones comunes del día a día y las muestra como complicados escenarios de ingeniería social. Finalmente, el libro desvela consejos y trucos que son información privilegiada de ingenieros sociales profesionales y, sí, incluso de delincuentes profesionales.

A veces me preguntan por qué querría yo revelar esta información. La respuesta es bastante sencilla: los "chicos malos" no se detienen por una limitación contractual o por su propia moral. No se rinden después de un intento fallido. Los maliciosos hackers no desaparecen porque a las empresas no les guste que se infiltren en sus servidores. Al contrario, la ingeniería social, los engaños de los empleados y el fraude en Internet son cada día más utilizados. Mientras que las

empresas de software van aprendiendo a fortalecer sus programas, los hackers y los ingenieros sociales maliciosos se dirigen a la parte más débil de la infraestructura: la gente. Su motivación tiene que ver con la rentabilidad sobre su inversión; ningún hacker que se respete a sí mismo va a dedicar 100 horas para lograr los mismos resultados que con un sencillo ataque en el que tarde una hora o menos.

Al final, la triste conclusión es que no hay forma de estar cien por cien seguros, a no ser que desenchufe todos los aparatos eléctricos y se vaya a vivir a las montañas. Ya que ésta no es una decisión muy práctica, ni parece demasiado divertida, este libro muestra maneras de ser más consciente de los ataques exteriores y explica los métodos que puede utilizar para protegerse de ellos. Mi lema es "seguridad a través de la formación". La formación es uno de los métodos infalibles para mantenerse seguro contra las amenazas crecientes de la ingeniería social y el robo de identidad. Kaspersky Lab, un proveedor líder de antivirus y software de protección, calculó que en 2009 se pusieron en circulación más de 100.000 muestras de malware a través de las redes sociales. En un informe reciente, Kaspersky estimó que "los ataques contra las redes sociales son diez veces más exitosos" que otros tipos de ataques.

El viejo dicho hacker "el conocimiento es poder" se aplica aquí: cuanto más conocimiento y comprensión se tengan de los peligros y amenazas que la ingeniería social puede suponer para cada consumidor y cada empresa y cuanto más se analice cada escenario de ataque, más fácil será mitigar, detener y protegerse de esos ataques. Ahí es donde entra en juego el poder de este conocimiento.

Por qué es tan valioso este libro

En el mercado hay muchos libros disponibles sobre seguridad, piratería informática, pruebas de seguridad e incluso ingeniería social. Muchos de estos libros proporcionan una información muy valiosa y consejos que ayudan a sus lectores. Incluso con toda esa información disponible, era necesario un libro que llevara la información sobre ingeniería social al siguiente nivel y que describiera estos ataques con detalle, explicándolos desde el punto de vista de quienes tienen malas intenciones.

Este libro no es una mera colección de historias alucinantes, ingeniosos pirateos o ideas disparatadas. Este libro desarrolla el primer marco de trabajo de ingeniería social del mundo. Analiza y disecciona la base misma de lo que caracteriza a un buen ingeniero social y proporciona consejos prácticos sobre cómo utilizar esas habilidades para mejorar la destreza de los lectores para evaluar la mayor debilidad: la "infraestructura humana".

El diseño

Este libro proporciona un enfoque único de la ingeniería social. Está estructurado en estrecha relación al minucioso entorno de ingeniería social que se encuentra en www.social-engineer.org/framework. Este ámbito conceptual explica las habilidades y las herramientas (a nivel físico, mental y de personalidad) que una persona debe poseer para ser un excelente ingeniero social.

Este libro opta por un enfoque directo, presentando primero el principio en el que se basa un tema, para después definir, explicar y analizarlo en detalle y mostrar su aplicación utilizando colecciones de historias reales y casos de estudio. No es tan sólo un libro sobre historias o trucos ingeniosos, sino un manual, una guía a través del oscuro mundo de la ingeniería social.

Durante el transcurso del libro puede encontrar muchos vínculos de Internet a historias o testimonios, así como vínculos a herramientas y otros aspectos de los temas tratados. Irán apareciendo ejercicios prácticos a lo largo del libro que están diseñados para ayudarle a dominar no sólo el entorno de la ingeniería social, sino también las habilidades para mejorar su comunicación cotidiana.

El libro le será de especial interés si es usted un experto en seguridad. Mientras vaya leyéndolo, espero hacerle suficiente hincapié en que la seguridad no es un trabajo a "tiempo parcial" y no es algo que pueda tomarse a la ligera. Como parece que los delincuentes y los ingenieros sociales maliciosos van a más en este mundo, los ataques sobre los negocios y sobre la vida personal parecen intensificarse. Naturalmente, todo el mundo quiere estar protegido, como evidencia el aumento en ventas de software e instrumentos de protección personal. Aunque estos elementos son importantes, la mejor protección es el conocimiento: seguridad a través de la formación. El único modo real de reducir el efecto de estos ataques es saber que existen, saber cómo son realizados y comprender el proceso de pensamiento y la mentalidad de las personas que harían algo así.

Cuando posee este conocimiento y comprende cómo piensan los maliciosos hackers, se enciende una bombilla. Esa luz proverbial iluminará los rincones antes oscuros y le permitirá ver claramente a los "chicos malos" acechantes. Cuando puede ver con antelación el modo en que se realizan estos ataques, puede preparar su empresa y sus asuntos personales para protegerlos.

Por supuesto, no estoy contradiciendo lo que dije antes; creo que no hay modo de estar seguro al cien por cien. Incluso los asuntos de alto secreto, fuertemente protegidos, pueden y de hecho han sido pirateados de maneras asombrosamente simples.

Lea la historia de un periódico de Otawa, Canadá, archivada en www.social-engineer.org/resources/book/TopSecretStolen.htm. Esta historia es muy interesante porque trata sobre unos documentos que acabaron en

las manos equivocadas. Y no eran unos documentos cualquiera, sino documentos de defensa de alto secreto que explicaban cosas como la localización de cercos de seguridad en la base de las fuerzas armadas de Canadá en Trenton, el plano de la Canadian Joint Incident Response Unit (Unidad de respuesta conjunta a incidentes canadiense) y otros. ¿Cómo se abrió una brecha semejante? Alguien arrojó los planos al cubo de la basura y alguien los encontró en el contenedor. Un simple vistazo a un contenedor pudo conducir a una de las brechas de seguridad más grandes del país.

Ataques simples aunque letales se lanzan cada día y evidencian el hecho de que la gente necesita formación; necesita cambiar el modo en que observan las políticas de contraseñas y el modo en que manejan los controles remotos a servidores; necesitan cambiar el modo en que manejan las entrevistas, las entregas y los empleados que son contratados y despedidos. Pero sin formación, la motivación para el cambio sencillamente no existe.

En 2003 el Computer Security Institute (Instituto de seguridad informática) llevó a cabo una inspección junto con el FBI y encontró que el 77 por 100 de las empresas entrevistadas declararon que un empleado descontento era la fuente de una brecha de seguridad importante. Vontu, la sección de prevención de pérdida de información de Symantec (`http://go.symantec.com/vontu/`), establece que 1 de cada 500 correos electrónicos contiene información confidencial. Éstos son algunos de los puntos más destacados de ese informe, citados de la Web `http://financialservices.house.gov/media/pdf/062403ja.pdf`:

- El 62 por 100 denunció incidentes en el trabajo que pudieron poner información de los clientes en riesgo de robo de identidad.
- El 66 por 100 afirma que sus compañeros de trabajo, no los hackers, suponen el mayor riesgo para la privacidad del consumidor. Sólo el 10 por 100 afirmó que los hackers eran la mayor amenaza.
- El 46 por 100 afirma que sería "fácil" o "extremadamente fácil" para los trabajadores eliminar información delicada de la base de datos de la empresa.
- El 32 por 100, más o menos uno de cada tres, no tiene conocimiento de políticas internas de la empresa para proteger la información de clientes.

Estas estadísticas son sorprendentes e inquietantes.

En capítulos posteriores, analizamos estas cifras más detalladamente. Los números evidencian un defecto importante en el modo en que se maneja la seguridad. Cuando hay formación (preferiblemente antes de que se produzca una brecha), la gente puede realizar cambios que pueden prevenir pérdidas no deseadas, dolor y daños económicos.

Sun Tzu dijo: "Si conoces a los demás y te conoces a ti mismo, ni en cien batallas correrás peligro". Cuánta verdad encierran estas palabras, pero el conocimiento es sólo la mitad de la batalla. Lo que define la sabiduría es actuar en base al conocimiento, no el conocimiento por sí solo.

Este libro es más efectivo utilizado como un manual o una guía a través del mundo de los ataques sociales, la manipulación social y la ingeniería social.

Lo que viene a continuación

Este libro está diseñado para cubrir todos los aspectos, herramientas y habilidades utilizados por ingenieros sociales profesionales y maliciosos. Cada capítulo profundiza en la ciencia y el arte de una habilidad de ingeniería social específica para mostrar cómo puede utilizarse, mejorarse y perfeccionarse.

La siguiente sección de este capítulo define la ingeniería social y el papel que juega en la sociedad de hoy en día, así como los diferentes tipos de ataques, incluyendo otras áreas de la vida donde la ingeniería social es utilizada con buenos propósitos. También explicará cómo un ingeniero social puede usar el entorno conceptual de la ingeniería social para planificar una auditoría o para mejorar sus propias habilidades.

En el capítulo 2 es donde realmente empieza la parte sustanciosa de las lecciones. La recopilación de información es la base de toda auditoría de ingeniería social. El lema del ingeniero social es: "Sólo soy tan bueno como la información que reúna". Un ingeniero social puede poseer todas las habilidades del mundo, pero si no tiene información sobre su objetivo, si no ha perfilado cada detalle íntimo, entonces es probable que fracase. La recopilación de información es el quid de toda acción de ingeniería social, aunque el don de gentes y la habilidad para improvisar pueden ayudarle a salir de alguna situación difícil. En la mayoría de los casos, cuanta más información reúna, mayores serán sus probabilidades de tener éxito.

Éstas son algunas de las cuestiones a las que responderé en ese capítulo:

- ¿Qué fuentes puede utilizar un ingeniero social?
- ¿Qué información es útil?
- ¿Cómo puede un ingeniero social recopilar y organizar esta información?
- ¿A qué nivel técnico debe llegar un ingeniero social?
- ¿Cuánta información es suficiente?

Después de analizar la recopilación de información, el siguiente tema tratado en el capítulo 2 es el diseño del modelo de comunicación. Este tema está íntimamente relacionado con el de la recopilación de información. Primero, ex-

plicaré el diseño del modelo de comunicación y cómo empezó como práctica. Después, el capítulo recorre los pasos necesarios para desarrollar y utilizar un modelo de comunicación adecuado. Subraya cómo un ingeniero social utiliza un determinado modelo sobre un objetivo y los beneficios de ponerlo en práctica en cada ocasión.

El capítulo 3 trata sobre las maniobras de obtención de información, el siguiente paso lógico. Realiza un examen en profundidad sobre cómo se utilizan las preguntas para lograr información, contraseñas y un conocimiento profundo del objetivo y su empresa. Aprenderá cómo se ejecuta una buena maniobra de obtención de información y lo importante que es planificarla previamente.

Este capítulo destaca también la importancia de llenar la mente de su objetivo con información para lograr que sus preguntas sean aceptadas fácilmente después. Al avanzar en esta sección, comprenderá que es fundamental llegar a ser bueno sonsacando información. También aprenderá a utilizar esta habilidad no sólo en su actividad en materia de seguridad, sino también en su vida diaria.

El capítulo 4 aborda un tema vital: el pretexto. Este denso tema es el punto crítico para muchos ingenieros sociales. El pretexto implica desarrollar el papel que el ingeniero social va a interpretar en el ataque a la empresa. Este papel debe ser realista y creíble. ¿Será el ingeniero social un cliente, un vendedor, alguien de soporte técnico, un empleado recién contratado?

El pretexto no sólo consiste en inventar el argumento, consiste también en desarrollar la apariencia de su personaje y el modo en que habla, camina y se comporta; decidir qué herramientas y conocimientos posee; dominar el paquete completo de forma que, cuando aborde a su objetivo, "sea" esa persona y no esté simplemente interpretando un papel.

Éstas son las cuestiones que se explican:

- ¿Qué es el pretexto?
- ¿Cómo se desarrolla un pretexto?
- ¿Cuáles son los principios de un pretexto exitoso?
- ¿Cómo puede un ingeniero social planificar y ejecutar un pretexto perfecto?

El siguiente paso puede llenar volúmenes enteros. Sin embargo, se debe explicar desde el punto de vista de un ingeniero social. En el capítulo 5 se tratan abiertamente temas muy polémicos, incluyendo el de los movimientos oculares (o pistas de acceso ocular). Por ejemplo, ¿cuáles son las diferentes opiniones de los profesionales sobre los movimientos oculares y cómo puede utilizarlos un ingeniero social? El capítulo también profundiza en la fascinante ciencia de las microexpresiones y sus implicaciones.

El capítulo 5 continúa con el análisis de la investigación, dando respuesta a estas preguntas:

- ¿Es posible utilizar las microexpresiones en el campo de la seguridad?
- ¿Cómo podría hacerse?
- ¿Qué aportan las microexpresiones?
- ¿Puede una persona entrenarse para aprender a percibir microexpresiones de manera automática?
- Después de completar el entrenamiento, ¿qué información se puede obtener a través de las microexpresiones?

Probablemente, uno de los temas más debatidos en el capítulo 5 es la programación neurolingüística (PNL). El debate mantiene a mucha gente indecisa sobre lo que es y cómo puede utilizarse. Por eso, presentamos una breve historia de la PNL así como el porqué de que sea tan controvertida. Usted puede decidir por sí mismo si la PNL es de utilidad en ingeniería social.

También se trata uno de los aspectos más importantes de la ingeniería social: aprender a hacer buenas preguntas (en persona o por teléfono), escuchar las respuestas y después hacer más preguntas. Los interrogatorios y las entrevistas son dos métodos que las fuerzas de orden público han utilizado durante años para manipular a los delincuentes para que confiesen, así como para resolver los casos más difíciles. En esta sección se pone en práctica el conocimiento obtenido en el capítulo 3.

También se explica cómo lograr una compenetración inmediata con los demás, una habilidad que, además, podrá utilizar en su vida diaria. El capítulo termina desarrollando mi propia investigación sobre "el desbordamiento de búfer humano": la idea de que la mente humana es muy parecida al software que los hackers atacan cada día. Aplicando ciertos principios, un ingeniero social experto puede invadir la mente humana e insertar en ella cualquier orden que desee.

Igual que los hackers reprograman un software para que ejecute un código, a la mente humana se le pueden dar ciertas instrucciones para, de cierta manera, "desbordar" al objetivo e insertarle instrucciones concretas. El capítulo 5 es una lección asombrosa sobre cómo utilizar algunas técnicas sencillas para dominar el modo en que piensan las personas. Muchas personas han pasado su vida investigando y probando cuáles son los aspectos que pueden influir en las personas. La influencia es una herramienta poderosa con muchas facetas. En este sentido, el capítulo 6 aborda los fundamentos de la persuasión. Los principios incluidos le guiarán para llegar a convertirse en un maestro de la persuasión.

Se presenta una breve discusión sobre los diferentes tipos de persuasión que existen y se proporciona ejemplos que ayudan a entender cómo puede utilizar estas facetas en la ingeniería social.

El análisis no termina aquí. Otro tema candente hoy en día es el conocido en sociología como "encuadre". Existen opiniones muy diversas sobre cómo utilizar el encuadre y este libro le muestra algunos ejemplos reales al respecto. Después, analizando cada uno, repasamos las lecciones aprendidas y estudiamos cómo puede practicar para aplicar el encuadre consigo mismo y en su actividad como ingeniero social.

Otro tema asombroso de la ingeniería social es la "manipulación":

- ¿Cuál es su propósito?
- ¿Cuáles son las motivaciones de los manipuladores?
- ¿Cómo puede utilizarse en ingeniería social?

El capítulo 6 ofrece todo lo que un ingeniero social necesita saber sobre el tema de la manipulación y sobre cómo aplicar esa técnica con éxito.

El capítulo 7 trata sobre las herramientas que pueden hacer más exitosa una auditoría de ingeniería social. Desde las herramientas físicas como las cámaras ocultas hasta el software de recopilación de información, cada sección analiza herramientas para ingenieros sociales probadas y examinadas.

Una vez que comprenda el marco conceptual de la ingeniería social, el capítulo 8 presenta algunos casos reales. He elegido dos testimonios excelentes del renombrado ingeniero social Kevin Mitnick. Analizo y disecciono estos ejemplos y después explico lo que se puede aprender de ellos e identifico los métodos que utilizó Mitnick. Además, planteo lo que podemos aprender de sus vectores de ataque y cómo pueden ser utilizados hoy. También presento y analizo algunos testimonios propios.

¿Qué guía de ingeniería social estaría completa sin explicar algunas de las formas en las que pueden disminuirse los ataques? El apéndice proporciona esta información. Respondo algunas preguntas habituales sobre la disminución de ataques y ofrezco algunos consejos excelentes para ayudarle a protegerse a sí mismo y a su organización de estos ataques maliciosos.

Esta visión general es sólo una muestra de lo que viene a continuación. Espero sinceramente que disfrute leyendo este libro tanto como yo he disfrutado escribiéndolo. La ingeniería social es una pasión para mí. Creo que hay ciertas características, ya sean aprendidas o inherentes, que pueden hacer de alguien un gran ingeniero social. También soy de los que opina que, con tiempo y energía suficientes, cualquiera puede aprender los distintos aspectos de la ingeniería social y después practicar estas habilidades para convertirse en un ingeniero social competente.

Los principios que aparecen en este libro no son nuevos; no va a encontrar una tecnología asombrosa que pueda cambiar el ámbito de la seguridad para siempre. No hay pociones mágicas. De hecho, los principios existen desde hace

tanto tiempo como las personas. Lo que hace este libro es combinar todas estas habilidades y localizarlas en un punto. Le proporciona una dirección clara sobre cómo practicar estas habilidades, así como ejemplos de situaciones reales en las que son utilizadas. Toda esta información puede ayudarle a lograr una verdadera comprensión de los temas tratados.

El mejor punto para empezar es con lo básico, respondiendo una pregunta fundamental: "¿Qué es la ingeniería social?"

Visión general de la ingeniería social

¿Qué es la ingeniería social?

Una vez le hice esta pregunta a un grupo de entusiastas de la seguridad y me sorprendieron mucho las respuestas que dieron:

"La ingeniería social es mentir a la gente para obtener información".

"La ingeniería social es ser un buen actor".

"La ingeniería social es saber cómo conseguir cosas gratis".

La Wikipedia la define como "el acto de manipular a la gente para llevar a cabo acciones o divulgar información confidencial. Aunque parecido a una estafa o un simple fraude, el término se aplica normalmente a las artimañas o engaños con el propósito de obtener información, llevar a cabo un fraude o acceder a un sistema informático; en la mayoría de los casos, el atacante nunca se enfrenta cara a cara con la víctima".

A pesar de que se ha ganado cierto mal nombre debido al exceso de sitios Web con reclamos del tipo de "pizza gratis", "café gratis" o "cómo ligar con chicas", en realidad los aspectos de la ingeniería social afectan a muchas aspectos del día a día.

El *Diccionario Webster* define "social" como "relativo o perteneciente a la vida, el bienestar y las relaciones de los seres humanos en una comunidad". También define la "ingeniería" como "el arte o la ciencia de llevar a aplicación práctica el conocimiento de las ciencias puras como la física o la química, en la construcción de máquinas, puentes, edificaciones, minas, embarcaciones y plantas químicas o artilugios ingeniosos; maniobrar".

Combinando ambas definiciones puede ver fácilmente que la ingeniería social es el arte o, mejor aún, la ciencia, de maniobrar hábilmente para lograr que los seres humanos actúen en algún aspecto de sus vidas.

Esta definición amplía los horizontes de los ingenieros sociales a todas partes. La ingeniería social es utilizada en la vida diaria, por ejemplo, en la forma en la que los niños consiguen que los padres atiendan a sus peticiones. Es utilizada por los profesores en el modo de interactuar con sus estudiantes y por los doctores,

abogados o psicólogos para obtener información de sus pacientes o clientes. Es claramente utilizada por las fuerzas de orden público y en las relaciones de pareja. En definitiva, es utilizada en cualquier interacción humana, desde los bebés hasta los políticos.

Me gusta llevar esta definición un paso más allá y afirmar que en realidad la ingeniería social es el acto de manipular a una persona para que lleve a cabo una acción que "puede ser o no" lo más conveniente para el "objetivo". Esto puede incluir obtener información, conseguir algún tipo de acceso o lograr que el objetivo realice cierta acción.

Por ejemplo, los médicos, los psicólogos y los terapeutas a menudo utilizan elementos que yo considero ingeniería social para "manipular" a sus pacientes para que realicen acciones que son buenas para ellos, mientras que un estafador utiliza elementos de la ingeniería social para convencer a su víctima para que realice acciones que le perjudican. Aunque el resultado es muy diferente, el proceso puede ser muy parecido. Un psicólogo utiliza una serie de preguntas bien intencionadas para ayudar a un paciente a llegar a la conclusión de que es necesario un cambio. De igual modo, un estafador utilizará preguntas capciosas para llevar a su objetivo a una posición vulnerable.

Ambos ejemplos son auténtica ingeniería social, pero tienen metas y resultados muy diferentes. La ingeniería social no consiste sólo en engañar a la gente o mentir o representar un papel. En una conversación que tuve con Chris Nickerson, un conocido ingeniero social de la serie de televisión *Tiger Team*, me dijo: "La verdadera ingeniería social no consiste sólo en creer que estás representando un papel, sino en que durante ese momento "eres" esa persona, eres ese papel, ésa es tu vida".

La ingeniería social no es una acción suelta, sino una recopilación de las habilidades que, cuando se unen, componen la acción, el ingenio y la ciencia que yo llamo ingeniería social. De la misma manera, una buena comida no es sólo un ingrediente, sino que se crea con la mezcla cuidadosa de varios ingredientes. Así imagino la ingeniería social; un buen ingeniero social es como un chef. Añada un pequeño toque de manipulación y un puñado de pretextos y ¡bam! Ya tiene el gran plato del ingeniero social perfecto.

Por supuesto, este libro aborda algunas de estas facetas, pero se centra principalmente en lo que puede aprender de las fuerzas del orden público, los políticos, los psicólogos e incluso los niños, para mejorar sus habilidades para realizar una auditoría y protegerse mejor a sí mismo. Analizar cómo un niño puede manipular a sus padres fácilmente otorga al ingeniero social el entendimiento sobre cómo funciona la mente humana. Observar cómo un psicólogo hace sus preguntas ayuda a ver como relajar a la gente. Observar cómo un agente de las fuerzas del orden realiza un interrogatorio proporciona un camino claro sobre cómo obtener información de un objetivo. Analizar cómo los políticos y los gobernantes estructuran

sus mensajes para lograr un mayor impacto puede dar una idea de lo que funciona y lo que no. Estudiar cómo se mete un actor en su papel puede abrirle los ojos al maravilloso mundo del pretexto. Diseccionando la investigación y el trabajo de algunas de las mejores mentes del campo de la microexpresión y la persuasión, puede ver cómo utilizar esas técnicas en la ingeniería social. Examinando las motivaciones de algunos de los mejores vendedores y expertos en persuasión del mundo, puede aprender cómo generar compenetración, hacer que la gente se sienta a gusto y cerrar tratos. Después, investigando y analizando el reverso de la moneda (los estafadores, los artistas del timo y los ladrones), podrá aprender cómo se unen estas habilidades para influir en la gente y conseguir que se dirijan hacia donde nunca lo hubieran hecho por sí solos.

Combine este conocimiento con la técnica de apertura de cerraduras, la destreza de los espías que utilizan cámaras ocultas y los métodos de los profesionales de la recopilación de información y tendrá un ingeniero social de talento.

No utilizará todas estas habilidades en cada ocasión ni tampoco conseguirá dominarlas todas. Sin embargo, comprendiendo "cómo" funcionan estas técnicas y "cuándo" deben utilizarse, cualquiera puede dominar la ciencia de la ingeniería social. Es cierto que hay personas con un talento natural, como Kevin Mitnick, que parece que puede convencer a cualquier persona para hacer cualquier cosa. Frank Abagnale Jr. tenía el talento natural de hacer creer a la gente que él era quien quería hacerles creer que era. Victor Lustig hizo algo increíble convenciendo a algunas personas de que tenía los derechos para vender la torre Eiffel, superándose sólo con su timo de Al Capone.

Estos ingenieros sociales y muchos otros como ellos muestran tener un talento natural o una falta de miedo que les permite intentar cosas que la mayoría de nosotros jamás nos atreveríamos a intentar. Desgraciadamente, en el mundo actual los maliciosos hackers mejoran continuamente sus técnicas para manipular a la gente y los ataques de ingeniería social maliciosa van en aumento. Dark Reading afirma en un artículo (`www.darkreading.com/database_security/security/attaks/showArticle.jhtml?articleID=226200272`) que las brechas de información han alcanzado entre 1 y 53 millones de dólares por brecha. Citando la investigación del Ponemon Institute, Dark Reading afirma que "Ponemon descubrió que los ataques vía Web, el código malicioso y los ataques internos maliciosos son los tipos de ataque más costosos, suponiendo más del 90 por 100 de todos los costes de delitos informáticos por organización y por año: un ataque a través de la Web cuesta 143.209 dólares; un ataque con código malicioso, 124.083 dólares; un ataque realizado por internos maliciosos, 100.300 dólares". El hecho de que los ataques internos estén entre los tres más costosos sugiere que las empresas deben ser más conscientes de la amenaza que supone la ingeniería social maliciosa, incluso a través de sus propios empleados.

Muchos de estos ataques podrían haberse evitado si la gente hubiera sido formada, porque hubiera podido actuar en base a esa formación. A veces, simplemente descubrir cómo piensa y actúa la gente maliciosa puede ser muy revelador.

Como ejemplo en una escala personal y mucho menor, hace poco discutía con una buena amiga sobre sus cuentas bancarias. Le preocupaba la posibilidad de ser víctima de una estafa o un pirateo. En el curso de la conversación empezamos a discutir sobre lo sencillo que es "adivinar" las contraseñas de la gente. Le dije que mucha gente utiliza la misma contraseña para todas sus cuentas; vi que se ponía pálida, reconociendo este comportamiento en sí misma. Le comenté que la mayoría de la gente utiliza contraseñas simplistas que combinan datos como el nombre de sus parejas o sus fechas de cumpleaños o de aniversario. Vi que se ponía todavía más pálida. Continué diciéndole que casi siempre la gente elige la "pregunta de seguridad" más simple, como "su apellido (o el de su madre) de soltera" y lo fácil que resulta averiguar esta información en Internet o con unas cuantas llamadas falsas.

Mucha gente incluso facilita esta información en sus cuentas de Blippy, Twitter o Facebook. Esta amiga no utiliza mucho las redes sociales, así que le pregunté si creía que recibiendo unas cuantas llamadas sería capaz de llegar a dar esta información. Por supuesto, dijo que no. Para ilustrar lo fácilmente que la gente entrega información personal, le dije que una vez en un restaurante vi un mantel individual de papel que tenía un cupón de descuento de 50 euros para un campo de golf local, una oferta muy atractiva. Para beneficiarse de esta oferta, sólo había que proporcionar el nombre, fecha de nacimiento y dirección y dar una contraseña para crear una cuenta que se recibiría por correo electrónico. No me di cuenta de todo esto hasta que alguien rellenaba el cupón y lo dejaba en la mesa. Todos los días se crean sitios Web para recoger información sensible.

Una llamada para una encuesta o una investigación rápida en Internet puede descubrir una fecha de nacimiento o de aniversario y, armado con esta información, tengo suficiente para crear una lista de ataque a contraseñas. Es más, una docena de sitios Web ofrecen registros de todo tipo de información personal de la gente por no más de 30 euros.

Comprender cómo piensan los ingenieros sociales maliciosos y cómo reaccionan los estafadores a cierta información y entender que los timadores lo intentan todo puede ayudar a la gente a ser más consciente de lo que sucede a su alrededor.

Un equipo de entusiastas de la seguridad y yo barrimos Internet recopilando historias que muestran muchos aspectos diferentes de la ingeniería social. Estas historias pueden ayudar a responder una pregunta fundamental: "¿Cómo se utiliza la ingeniería social con el paso del tiempo?". Con ellas también podemos determinar qué lugar ocupa la ingeniería social y cómo se utiliza maliciosamente.

La ingeniería social y su lugar en la sociedad

Como ya hemos explicado, la ingeniería social puede utilizarse en muchas facetas de la vida, pero no todos estos usos son maliciosos o negativos. Muchas veces la ingeniería social puede utilizarse para motivar a una persona para realizar una acción que es buena para ella. ¿Cómo?

Piense esto: John necesita perder peso. Sabe que su salud es mala y que tiene que hacer algo al respecto. Todos los amigos de John tienen sobrepeso también. Incluso hacen chistes sobre las alegrías de tener sobrepeso y dicen cosas como "me encanta no tener que preocuparme por mi figura". Por una parte, esto es un aspecto de la ingeniería social. Es una prueba social o consenso, donde lo que se considera aceptable está determinado por quienes están alrededor. Como la gente más cercana a John considera que el sobrepeso es aceptable, es más fácil para John aceptarlo también. Sin embargo, si uno de los amigos de John pierde peso y en vez de criticar a los demás decide intentar ayudarlos, existe la posibilidad de que cambie la estructura mental de John sobre su peso y empiece a pensar que adelgazar es posible y bueno para él.

Esto es, en esencia, ingeniería social. Para que pueda ver cómo encaja la ingeniería social en la sociedad y en la vida diaria, las siguientes secciones muestran algunos ejemplos de ingeniería social, timos y manipulaciones y un análisis de cómo funcionaron.

El timo 419

El timo 419, más conocido como el timo nigeriano, ha crecido hasta convertirse en una epidemia. Puede encontrar una historia archivada y un artículo sobre este timo en `www.social-engineer.org/Wiki/archives/ConMen-Scam-NigerianFee.html`.

Básicamente, a la víctima le llega un correo electrónico (o, últimamente, una carta) diciéndole que ha sido elegida para un trato muy lucrativo y todo lo que tiene que hacer es ofrecer un poco de ayuda. Si la víctima ayuda al remitente de la carta a extraer una gran suma de dinero de unos bancos extranjeros, podrá quedarse con un porcentaje. Cuando la víctima se confía y accede a participar, surge un problema que provoca que la víctima tenga que pagar una pequeña suma de dinero. Después de pagar esa suma, surge otro problema y debe pagarse otra cantidad. Cada problema que surge siempre es "el último" con "una última cantidad de dinero" y este proceso puede alargarse durante meses. La víctima nunca ve ningún dinero y pierde entre 10.000 y 50.000 euros en el proceso. Lo que hace esta estafa aún más

increíble es que, en el pasado, algunas víctimas han denunciado la existencia de documentos oficiales, papeles con membrete e incluso reuniones cara a cara.

Recientemente, ha surgido una variante de este timo, en el que las víctimas reciben un cheque real. Los timadores prometen una enorme cantidad de dinero y sólo piden una pequeña parte por su esfuerzo. Si la víctima transfiere una pequeña cantidad (en comparación a lo que va a ganar) de 1.000 euros, cuando reciba el cheque puede depositarlo y quedarse con la diferencia. El problema es que el cheque que recibe es un fraude y cuando la víctima va a hacerlo efectivo, se encuentra con que debe afrontar cargos por cheque fraudulento y multas, en algunos casos "después" de que la víctima haya enviado dinero al estafador.

Este timo tiene éxito porque juega con la avaricia de la víctima. ¿Quién no daría 1.000 euros por recibir un millón o incluso 100.000 euros? Muchas personas lo harían. Cuando a la gente se le presentan documentos oficiales, pasaportes, recibos e incluso van a oficinas oficiales con "personal gubernamental", se convencen de que es cierto y pueden llegar muy lejos para completar el trato. El compromiso y la consistencia juegan un papel importante en este timo. En capítulos posteriores, explico estos aspectos y entonces verá por qué este timo es tan poderoso.

El poder de la escasez

El artículo archivado en `ww.social-engineer.org/Wiki/archives/Governments/Governments-FoodElectionWeapon.html` habla sobre un principio llamado "escasez".

Escasez es cuando se le dice a la gente que las existencias de algún producto que necesitan o que quieren están limitadas y para conseguirlo deben cumplir algún requisito o realizar algún tipo de acción. Muchas veces ni siquiera se menciona el requisito, lo que se hace es mostrar cómo obtiene recompensas la gente que está actuando "adecuadamente".

El artículo habla sobre la utilización de la comida para ganar las elecciones en Sudáfrica. Cuando un grupo o una persona no apoyan al líder "adecuado", los alimentos empiezan a escasear y se quita el trabajo a la gente para dárselo a otras personas que sí están dando su apoyo. Cuando la gente ve funcionar este mecanismo, no lleva mucho tiempo convencerla.

Ésta es una forma de ingeniería social muy maliciosa y dañina pero, aun así, se puede aprender algo de ella: a menudo la gente quiere lo que es escaso y haría cualquier cosa si se le hace creer que ciertas acciones pueden provocar que pierda esos productos. Lo que hace algunos casos todavía peores, como en el ejemplo anterior, es que un gobierno tome algo necesario para la vida y lo haga "escaso" y sólo disponible para sus seguidores. Una táctica de manipulación maliciosa, pero muy efectiva.

El Dalai Lama y la ingeniería social

El interesante artículo archivado en www.social-engineer.org/Wiki/archives/Spies/Spies-DalaiLama.html detalla un ataque al Dalai Lama realizado en 2009.

Un grupo de hackers chinos querían acceder a los servidores y archivos de la red del Dalai Lama. ¿Qué métodos se utilizaron en este exitoso ataque?

Los atacantes convencieron al personal de la oficina del Dalai Lama para descargar y abrir software malicioso en sus servidores. Este ataque es interesante porque combina el pirateo tecnológico con la ingeniería social.

El artículo señala: "El software se adjuntó a correos electrónicos que supuestamente procedían de colegas o contactos del movimiento tibetano, según el investigador Ross Anderson, profesor de ingeniería de seguridad del laboratorio informático de la Universidad de Cambridge, citado el lunes en el *Washington Times*. El software robó contraseñas y otros datos que dieron a los hackers acceso al sistema de correo electrónico de la oficina y a toda la documentación almacenada en los ordenadores".

Se utilizaron la manipulación y otros vectores de ataque habituales como el *phishing* (la práctica de enviar correos electrónicos con mensajes tentadores y vínculos o archivos que deben ser abiertos para recibir más información; a menudo esos vínculos o archivos conducen a cargas destructivas) o la explotación de vulnerabilidades.

Este ataque puede funcionar y funciona contra importantes empresas e incluso gobiernos. Este ejemplo es sólo uno de entre un gran número de ellos donde estas formas de ataque causaron grandes daños.

Robo de empleados

El tema del robo de empleados puede llenar volúmenes enteros, especialmente a la luz de la sorprendente estadística que se puede ver en www.social-engineer.org/wiki/archives/DisgruntledEmployees/DisgruntledEmployees-EmployeeTheft.html, que indica que más del 60 por 100 de los empleados entrevistados admitieron haber cogido información de algún tipo de sus empleadores.

Muchas veces esta información se vende a la competencia (como sucedió en esta historia de un empleado de Morgan Stanley: www.social-engineer.org/wiki/archives/DisgruntledEmployees/DisgruntledEmployees-Morgan Stanley.html). Otras veces lo que roban los empleados es tiempo u otros recursos; en algunos casos, un empleado descontento puede causar un gran daño.

En una ocasión, hablé con un cliente sobre las políticas de despido de empleados, asuntos como desactivar llaves electrónicas, desconectar cuentas de red y acompañar a los empleados despedidos fuera del edificio. La empresa consideraba que todo el mundo allí era parte de la "familia" y que no era necesario aplicar esas políticas.

Desgraciadamente, llegó el día de despedir a "Jim", una de las personas de más alto rango de la empresa. El "despido" fue bien; fue amigable y Jim fue comprensivo. Una cosa que la empresa hizo correctamente fue llevar a cabo el despido a última hora de la jornada para evitar el bochorno o cualquier tipo de distracción. Hubo un apretón de manos y entonces Jim hizo la fatídica pregunta: "¿Puedo tomarme una hora para limpiar mi mesa y sacar algunas fotos personales del ordenador? Devolveré mi llave electrónica al guardia de seguridad antes de irme".

Al tener buenas sensaciones después de la reunión, todos estuvieron rápidamente de acuerdo y se fueron entre alegres sonrisas. Entonces Jim se fue a su despacho, empaquetó sus objetos personales, sacó las fotos y otros datos de su ordenador, se conectó a la red y limpió el equivalente a 11 servidores en información: registros de contabilidad, nóminas, facturas, órdenes, historiales, gráficos y mucho más, todo borrado en cuestión de minutos. Jim devolvió la llave electrónica como prometió y tranquilamente abandonó el edificio sin dejar pruebas de que fue él quien llevo a acabo este ataque.

A la mañana siguiente recibí una llamada del dueño de la empresa describiendo la carnicería que dejó tras de sí el ex empleado. El cliente esperaba una solución milagrosa, pero no tuvo más opción que intentar recuperar lo que fuera posible y volver a empezar a partir de las copias de seguridad que tenían una antigüedad de más de dos meses.

Un empleado descontento al que se deja actuar libremente puede ser más devastador que un equipo de hackers decididos y experimentados. La pérdida estimada sólo en empresas de Estados Unidos por robos de empleados es del orden de 15.000 millones de dólares.

Estas historias deben plantear la cuestión de cuántas categorías diferentes de ingeniería social existen en el mundo y cómo pueden ser clasificadas.

DarkMarket y Master Splynter

En 2009 salió a la luz una historia sobre un grupo clandestino llamado DarkMarket, el llamado eBay para delincuentes; un grupo muy compacto que intercambiaba números de tarjetas de crédito robados, herramientas para robos de identidad y los elementos necesarios para fabricar credenciales falsas y otros productos.

Un agente del FBI llamado J. Keith Mularski se infiltró de incógnito en el sitio Web de DarkMarket. Después de un tiempo, hicieron al agente Mularski administrador del sitio Web. A pesar de que muchos intentaron desacreditarle, se mantuvo más de tres años como administrador del sitio.

Durante todo este tiempo, Mularski tuvo que vivir como un hacker, hablar y actuar como ellos y pensar como ellos. Su pretexto era ser un malicioso *spammer* y tuvo la capacidad y la inteligencia suficientes para llevarlo a cabo. Su pretexto y sus habilidades de ingeniería social dieron sus frutos, porque el agente Mularski se infiltró en DarkMarket como el famoso Master Splynter y después de tres años su trabajo fue clave para desarticular una enorme trama de robo de identidad.

La operación encubierta de ingeniería social de tres años de duración consiguió 59 arrestos y evitó más de 70 millones de dólares en fraudes bancarios. Esto es un ejemplo de cómo puede utilizarse la ingeniería social para buenas causas.

Los distintos tipos de ingenieros sociales

Como hemos indicado previamente, la ingeniería social puede adoptar muchas formas. Puede ser maliciosa o amigable, puede crear o destruir. Antes de continuar, repasemos brevemente los diferentes tipos de ingenieros sociales y una descripción corta de cada uno:

- **Hackers:** Los proveedores de software van logrando crear software cada vez más "blindado" o más difícil de forzar. Como los hackers se encuentran con un software más seguro y los vectores de ataque a software y redes, como el pirateo remoto, son cada vez más difíciles, los hackers están acudiendo a las técnicas de la ingeniería social. Utilizando a menudo una combinación de hardware y técnicas personales, los hackers están utilizando la ingeniería social tanto en grandes ataques como en pequeñas brechas.
- **Probadores de seguridad:** Estos profesionales aprenden y utilizan las técnicas de los hackers para ayudar a garantizar la seguridad de sus clientes. Los probadores de seguridad poseen las habilidades de los piratas informáticos, pero nunca utilizan esa información para su beneficio personal o para dañar al objetivo.
- **Espías:** Para los espías la ingeniería social es un modo de vida. Emplean a menudo todos los aspectos del entorno conceptual de la ingeniería social (abordados más adelante en este capítulo) y son expertos en esta ciencia. Aprenden diferentes métodos para "engañar" a sus víctimas haciéndoles creer que son alguien o algo que no son. Además de aprender el arte de la ingeniería social, muchas veces aumentan su credibilidad aprendiendo un poco o incluso mucho del negocio o gobierno contra el que maquinan.

- **Ladrones de identidad:** El robo de identidad es el uso de datos como el nombre de una persona, números de cuentas bancarias, direcciones, fechas de nacimiento y números de la seguridad social sin el conocimiento del propietario. Este delito puede variar desde ponerse un uniforme para caracterizarse como alguien hasta estafas mucho más elaboradas. Los ladrones de identidad emplean muchos aspectos de la ingeniería social y según pasa el tiempo parecen más envalentonados e indiferentes ante el sufrimiento que causan.
- **Empleados descontentos:** Una vez que el empleado está descontento, muchas veces entra en una relación de enemistad con su empleador. Suele ser una situación unilateral, ya que el empleado normalmente ocultará su disgusto para no arriesgar su empleo. Sin embargo, cuanto más descontento esté, más sencillo le resultará justificar actos de vandalismo, robo u otros delitos.
- **Artistas del timo:** Los timadores y estafadores apelan a la avaricia de la gente o a otros principios y a sus deseos de "sacar tajada". Los artistas del timo o estafadores dominan la habilidad de leer a las personas y reconocen pequeñas señales que hacen de alguien una buena "marca". También son habilidosos creando situaciones que parecen oportunidades inigualables para la marca.
- **Agentes de recursos humanos:** Estos profesionales también deben dominar varios aspectos de la ingeniería social. Tienen que dominar las maniobras de obtención de información y muchos de los principios psicológicos de la ingeniería social; además, son expertos no sólo en leer a las personas sino también en comprender qué es lo que motiva a la gente. A menudo, el agente de recursos humanos debe tomar en consideración y satisfacer no sólo a la persona que está buscando trabajo, sino a la persona que ofrece el trabajo.
- **Vendedores:** Parecidos a los agentes de recursos humanos, los vendedores deben dominar muchas habilidades humanas. Muchos gurús de las ventas afirman que un buen vendedor no manipula a la gente sino que utiliza sus habilidades para descubrir cuáles son las necesidades de la gente para después tratar de satisfacerlas. El arte de las ventas maneja muchas técnicas como la recopilación de datos, las maniobras de obtención de información, la influencia, los principios psicológicos y muchas otras habilidades humanas.
- **Gobiernos:** No siempre son vistos como ingenieros sociales, pero los gobiernos utilizan la ingeniería social para controlar el mensaje que envían y a las personas que gobiernan. Muchos gobiernos utilizan la prueba social, la autoridad y la escasez para asegurarse de que sus súbditos estén bajo

control. Este tipo de ingeniería social no siempre es negativo, porque algunos de los mensajes que los gobiernos envían son por el bien de la gente y utilizar ciertos elementos de la ingeniería social puede hacer el mensaje más atractivo y más ampliamente aceptado.

- **Médicos, psicólogos y abogados:** Aunque las personas con estas carreras no parecen encajar en la misma categoría que muchos de los otros ingenieros sociales, este grupo emplea los mismos métodos usados por otros grupos de la lista. Deben realizar maniobras para obtener información y tácticas adecuadas en sus entrevistas e interrogatorios, además de muchos o todos los principios de la ingeniería social para manipular a sus "objetivos" (pacientes o clientes) en la dirección que ellos desean.

Parece que se puede encontrar la ingeniería social o algún aspecto de ella en cualquier campo. Por eso, sostengo firmemente que la ingeniería social es una ciencia. Existen ecuaciones establecidas que permiten a una persona "sumar" elementos de la ingeniería social para llegar a su meta. En el ejemplo de un estafador, piense en una ecuación como ésta: pretexto + manipulación + avaricia = ingeniería social aplicada sobre la víctima.

En cada situación, saber qué elementos van a funcionar es la parte más difícil, pero aprender cómo utilizar esos elementos es donde entra en juego la técnica. Éste fue el pensamiento de base para desarrollar el entorno conceptual de la ingeniería social. Este ámbito ha revolucionado el modo en que la ingeniería social es analizada, como se explica en la siguiente sección.

El entorno conceptual de la ingeniería social y cómo utilizarlo

A través de la investigación y la experiencia he tratado de perfilar los elementos que componen un ingeniero social. Cada uno de estos elementos define una parte de la ecuación que es igual a un ingeniero social completo. Estos aspectos no son inamovibles; de hecho, desde su estado original hasta ahora el entorno ha ido creciendo.

El propósito es ofrecer la información suficiente para que cualquiera pueda desarrollar estas habilidades. El entorno no está diseñado para ser un recurso que incluya toda la información de cada capítulo. Por ejemplo, la parte del capítulo 5 que trata sobre las microexpresiones se basa, por un lado, en investigaciones de algunas de las mentes más privilegiadas del sector y, por otro, en mi experiencia utilizando esa información. Bajo ningún concepto pretende reemplazar los cincuenta años de investigación de genios como el doctor Paul Ekman.

Mientras vaya leyendo el libro, verá que, utilizando las técnicas que incluye, no sólo mejorará sus prácticas de seguridad, sino también su mentalidad sobre cómo mantenerse seguro, cómo comunicarse más plenamente y cómo entender el modo de pensar de la gente.

Diríjase al índice para hacerse una idea clara del entorno conceptual o consúltelo *on-line* en `www.social-engineer.org/framework`. A primera vista, puede resultar intimidante, pero en este libro encontrará un análisis de cada tema que le permitirá aplicar, mejorar y construir estas habilidades.

El conocimiento es poder, es cierto. En este sentido, la formación es la mejor defensa contra la mayoría de los ataques de ingeniería social. Incluso en aquéllos contra los que el conocimiento no puede protegerle al cien por cien, conocer en detalle estos ataques le mantendrá alerta. La formación puede ayudarle a mejorar sus propias habilidades y a estar vigilante.

No obstante, además de formación, necesita práctica. Este libro no ha sido diseñado para leerse sólo una vez; fue diseñado para ser una guía de estudio. Puede practicar y adaptar cada sección a sus necesidades. El entorno es progresivo en el sentido de que está ideado del mismo modo en que se prepara un ataque de ingeniería social. Cada sección trata el siguiente tema en el orden en que un ingeniero social emplearía esa técnica en sus fases de planificación y captación.

Muestra cómo debe perfilarse un ataque. Después de la planificación del ataque, las habilidades que se necesitan pueden ser estudiadas, mejoradas y practicadas antes de su utilización.

Suponga, por ejemplo, que está planificando una auditoría de ingeniería social a una empresa que quiere comprobar si usted puede acceder al cuarto del servidor y robar información.

Puede que su plan de ataque sea fingir que es alguien del servicio técnico que necesita acceso al cuarto del servidor. Necesitará reunir información, puede que incluso tenga que buscarla en un contenedor.

Después, con el pretexto de ser el técnico, puede utilizar cámaras ocultas y practicar las señales faciales y vocales para tener el aspecto de un técnico de asistencia y actuar y hablar como uno.

Si localiza las empresas de servicio técnico que utiliza su cliente puede que tenga que reunir información al respecto. ¿Con quién contacta normalmente su cliente? ¿Cuáles son los nombres de los empleados con los que interactúan? El ataque debe planificarse adecuadamente.

Sin embargo, este libro no es sólo para quienes realizan auditorías. Muchos lectores tienen curiosidad por conocer los ataques, no porque tengan que proteger a una empresa, sino porque tienen que protegerse a sí mismos. No conocer el modo en que piensa un ingeniero social malicioso puede hacer que sufra un ataque.

Estudiantes universitarios del campo de la seguridad también han utilizado el entorno conceptual. La información que proporciona dibuja un camino realista para estos métodos de ataque y permite al lector estudiarlos en profundidad.

Normalmente, esta información también puede ayudarle a mejorar su habilidad para comunicarse en su vida diaria. Aprender a leer las expresiones faciales o cómo utilizar preguntas para relajar a la gente y sonsacar respuestas positivas puede mejorar su habilidad para comunicarse con su familia y amigos. Puede ayudarle a convertirse en alguien que sabe escuchar y que es más consciente de los sentimientos de los demás.

Ser capaz de leer el lenguaje corporal, las expresiones faciales y los tonos de voz también puede mejorar su habilidad para ser un comunicador efectivo. Comprender cómo protegerse a sí mismo y a sus seres queridos le enriquecerá y le hará más consciente del mundo que le rodea.

Resumen

Como en cualquier libro, la información contenida aquí sólo es útil si la pone en práctica. Cuanto más practique, mayor será su éxito dominando estas técnicas. Anteriormente, expuse cómo la ingeniería social es parecida a dominar el arte de la cocina. Combinando los ingredientes adecuados en la cantidad adecuada puede lograr una comida estimulante y llena de sabor. La primera vez que intente cocinar puede que la comida tenga demasiada sal o puede que le falte sabor, pero no por eso tirará la toalla, seguirá intentándolo hasta que le salga bien. Con la ingeniería social ocurre lo mismo. Algunas de las habilidades necesarias vendrán de forma más natural y otras puede que resulten más difíciles.

Si un tema concreto le resulta difícil de comprender, no se rinda y no asuma que no puede aprenderlo. Todo el mundo puede aprender y utilizar estas habilidades con la cantidad adecuada de esfuerzo y trabajo.

También tenga en cuenta que, igual que en una receta culinaria, en una actuación de ingeniería social hay muchos "ingredientes". Puede que el primer ingrediente cobre más sentido una vez que haya avanzado un poco más. Algunas habilidades, como "el desbordamiento de búfer humano" tratado en el capítulo 5, sólo tendrán sentido después de dominar algunas de las otras habilidades explicadas en el libro.

A pesar de esto, continúe practicando y asegúrese de hacer investigación extra en los temas en los que necesite más claridad. Ahora, empezamos a cocinar. Su "receta" empieza en el próximo capítulo con el primer ingrediente, la recopilación de información.

2. La recopilación de información

La guerra es, en un noventa por ciento, información.
Napoleón Bonaparte

Se dice que no hay información irrelevante. Esas palabras son ciertas en lo que se refiere a este capítulo sobre la recopilación de información. En términos de ingeniería social, hasta el menor detalle puede conducir a una brecha beneficiosa para el éxito de sus propósitos.

Mi buen amigo y mentor Mati Aharoni, que ha sido probador de seguridad profesional durante más de una década, cuenta una historia que explica muy bien este punto. Le encargaron la tarea de intentar acceder a una empresa que apenas tenía rastro en Internet. Ya que la empresa ofrecía muy pocas vías por las que penetrar, conseguir acceder a ella constituía un auténtico reto.

Mati comenzó barriendo Internet en busca de algún detalle que le condujera a un camino de entrada. En una de sus búsquedas localizó a un alto directivo de la empresa que utilizaba su correo electrónico corporativo en un foro de coleccionistas de sellos y que mostraba mucho interés por los sellos de los años 50. Rápidamente, Mati registró una URL, algo así como `www.stampcollection.com` y después buscó unas cuantas fotos de sellos antiguos en Google. Creó un sencillo sitio

Web para mostrar su "colección de sellos" y después envió un correo electrónico al directivo de la empresa:

Estimado señor:

He visto en `www.forum.com` *que le interesan los sellos de los años cincuenta. Mi abuelo falleció recientemente y me dejó una colección de sellos que me gustaría vender. He creado un sitio Web a tal efecto; si quisiera ver la colección, visite por favor* `www.stampcollection.com`.

Gracias,

Mati

Antes de enviar el correo electrónico al objetivo, quería asegurarse de lograr el máximo impacto. Consiguió el número de teléfono del directivo a través del foro y le dejó un mensaje en el buzón de voz: "Buenos días señor, soy Bob. Vi su mensaje en `www.forum.com`. Mi abuelo acaba de fallecer y me ha dejado unos cuantos sellos de los años cincuenta y sesenta. He hecho unas fotos y he creado un sitio Web. Si está interesado puedo enviarle el vínculo para que eche un vistazo".

El objetivo estaba ansioso por ver la colección y aceptó de buena gana el correo electrónico. Mati le envió el correo y esperó a que hiciera clic en el vínculo. Lo que hizo Mati fue incrustar un marco malicioso en el sitio Web. Este marco contenía un código que explotaría una vulnerabilidad, muy conocida entonces, del navegador Internet Explorer y daría a Mati control sobre el ordenador del objetivo.

La espera no fue larga: en cuanto el directivo recibió el correo electrónico hizo clic en el vínculo poniendo a su empresa en peligro.

Una minúscula cantidad de información (el correo electrónico corporativo que el directivo utilizaba para buscar sellos) fue lo que condujo a la situación de peligro. Ninguna información es irrelevante. Con esa idea en mente, surgen algunas preguntas en relación a la recopilación de información:

- ¿Cómo puede recopilar información?
- ¿Qué fuentes de recopilación de información existen para ingenieros sociales?
- ¿Qué puede deducir de esos datos para retratar a sus objetivos?
- ¿Cómo puede localizar, almacenar y catalogar toda esta información para facilitar su utilización?

Éstas son sólo algunas de las preguntas que tendrá que responder para conseguir que la recopilación de información sea efectiva. Con el maremágnum de redes sociales que existe, la gente puede compartir fácilmente cualquier aspecto de su

vida con quien quiera, haciendo que algunos datos potencialmente perjudiciales estén más disponibles que nunca. Este capítulo se centra en los principios de la recopilación de información presentando ejemplos sobre cómo puede utilizarse en ingeniería social y los devastadores efectos que tiene sobre la seguridad personal la información que la gente hace pública en la Web.

Muchas de las habilidades o los métodos que un ingeniero social puede utilizar provienen de otros campos. Un área excelente para la recopilación de información es el de las ventas. Los vendedores suelen ser muy habladores y fáciles de tratar y suelen ser muy buenos reuniendo información sobre aquéllos con quienes interactúan.

En una ocasión, leí un libro sobre ventas en el que el autor animaba a los vendedores a reunir referencias de los compradores. Decía algo así: "¿Puede indicarme alguna persona que usted crea que puede beneficiarse de este producto tanto como usted?". Expresarse de forma sencilla puede ayudar a que una persona se abra y le remita a su familia, amigos e incluso a sus compañeros de trabajo. "Cosechar" o reunir esta información y almacenarla permite a los vendedores tener lo que ellos llaman "pistas calientes" a las que visitar. Una pista caliente es una persona con la que tienen una vía de acceso, una manera de acceder a ella evitando hacer lo que ellos denominan una llamada "a puerta fría".

Ahora el vendedor puede ponerse en contacto con esas referencias y decir algo como: "Acabo de estar en casa de Jane, su vecina, y ha comprado la póliza Premium. Ha estudiado las prestaciones y ha decidido pagar un año por adelantado. Me ha comentado que quizá a usted le interesaría el mismo tipo de cobertura. ¿Tiene un minuto para que le muestre el producto que ha contratado Jane?".

Estas técnicas utilizadas por los vendedores son a menudo imitadas por los ingenieros sociales. Por supuesto, un ingeniero social no pide referencias, pero piense en la cantidad de información que hay circulando en esta conversación. El vendedor recoge información de su cliente actual, después transmite esa información de un modo que haga al nuevo objetivo más susceptible de escucharle y dejarle entrar en su casa. Además, lanzando insinuaciones sobre lo que el primer cliente ha comprado y utilizando expresiones como "Premium" y "por adelantado", el vendedor está "cargando" al nuevo objetivo con las palabras clave que va a utilizar con él enseguida. Esta técnica es efectiva porque genera confianza, utiliza la familiaridad y consigue que el objetivo se sienta cómodo con el vendedor o el ingeniero social, eliminando las barreras que normalmente habría en su mente. Este capítulo y el siguiente profundizarán en estos temas.

Como ingeniero social, es de vital importancia comprender ambos ángulos para utilizarlos después de forma efectiva. Volviendo al ejemplo del chef del capítulo 1, un buen chef lo sabe todo sobre cómo conseguir los productos de mejor calidad, las verduras más frescas y las mejores carnes. Conoce muy bien los ingredientes que componen la receta, pero a no ser que se usen las cantidades correctas, la co-

mida puede estar sosa o demasiado fuerte o sencillamente estar incomible. Saber que una receta necesita sal no le convierte en chef, pero saber cómo combinar los ingredientes adecuados en las cantidades correctas puede ayudarle a dominar el arte de la cocina. Un ingeniero social debe dominar los tipos y cantidades de técnicas que hay que utilizar (la "receta"). Cuando lo logre, se convertirá en un maestro de la ingeniería social. Este capítulo ayuda a encontrar ese equilibrio. El primer ingrediente en cualquier receta para un ingeniero social es la información (detallado en la sección siguiente). Cuanto mayor sea la calidad de los datos, mayores serán las probabilidades de tener éxito. Este capítulo comienza explicando cómo recopilar información. Después, pasa a discutir las fuentes que pueden utilizarse para esta tarea. El capítulo no estaría completo sin explicar cómo unirlo todo y cómo utilizar estos recursos como ingeniero social.

Recopilar información

Recopilar información es como construir una casa. Si intenta empezar por el tejado, lo más probable es que fracase. Una buena casa se construye empleando unos cimientos sólidos y edificando a partir de ahí, del suelo hacia arriba. Al recopilar información puede sentirse abrumado intentando organizar y utilizar el material, por lo que es buena idea crear un archivo o iniciar una aplicación de recopilación para reunir los datos.

Existen muchas herramientas que ayudan a recopilar y utilizar la información. Para realizar pruebas de seguridad y auditorías de ingeniería social utilizo una distribución Linux llamada BackTrack específicamente diseñada con este propósito. BackTrack, como casi todas las distribuciones Linux, es de software libre y fuente abierta. Quizá su mayor ventaja sea que contiene más de 300 herramientas diseñadas para ayudar en auditorías de seguridad.

Todas las herramientas de BackTrack son también de software libre y fuente abierta. La alta calidad de las herramientas de BackTrack es especialmente atractiva; muchas de ellas rivalizan o incluso sobrepasan a herramientas que cuestan un ojo de la cara. Dos instrumentos de BackTrack especialmente útiles para la recopilación y almacenaje de información son Dradis y BasKet. En las siguientes secciones se explican rápidamente ambos.

La utilización de BasKet

BasKet tiene una funcionalidad parecida a Notepad, pero más bien se parece a un Notepad con superpoderes. Kelvie Wong mantiene actualmente el programa que puede encontrarse gratis en BackTrack o en `http://basket.kde.org/`.

En el sitio Web se encuentran las instrucciones para instalar BasKet. Una vez instalado, BasKet es fácil de usar y tiene una interfaz sencilla. Como muestra la figura 2.1, la interfaz es fácil de comprender. Crear una nueva "cesta" para contener información es tan sencillo como hacer clic con el botón derecho en el lado izquierdo de la pantalla y seleccionar New Basket (Nueva cesta).

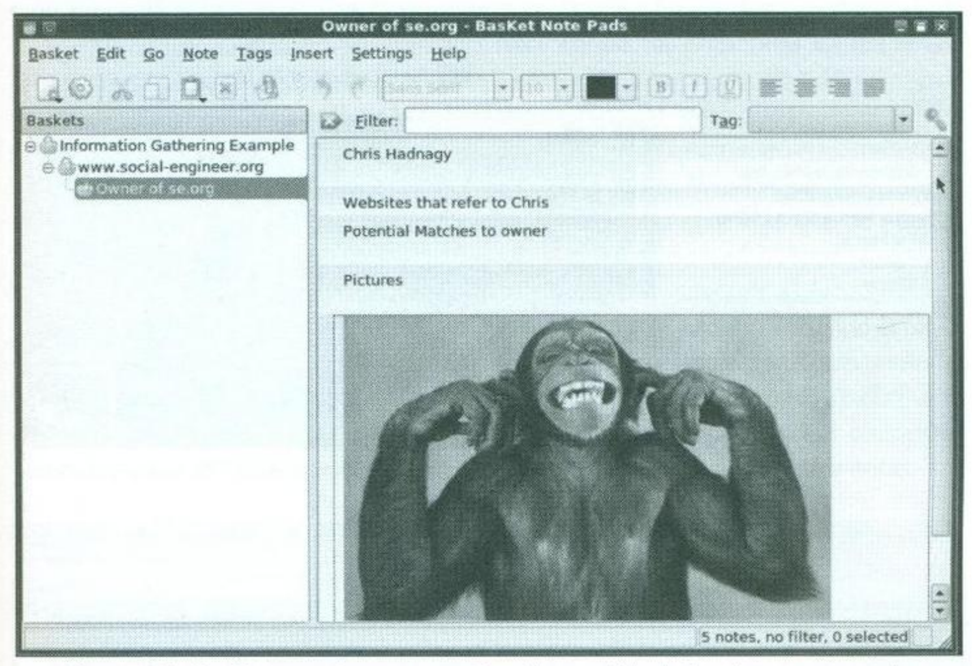


Figura 2.1. *BasKet permite una organización sencilla de los datos encontrados durante la recopilación de información.*

Una vez creadas las cestas nuevas, ya no hay límite. Puede copiar y pegar datos, incluir capturas de pantalla en la cesta o incluso relacionar OpenOffice o cualquier otro tipo de tabla, gráfico u otras utilidades.

Añadir una captura de pantalla puede hacerse de varias maneras. La más sencilla es copiar la imagen y después hacer clic con el botón derecho en la nueva cesta y hacer clic en Paste (Pegar).

Como muestra la figura 2.1, añadir imágenes es fácil y además la imagen aparece inmediatamente. Las notas pueden escribirse o pegarse simplemente haciendo clic en la cesta y empezando a escribir.

En una auditoría de seguridad normal, lo interesante de BasKet es el modo en que cataloga los datos y los muestra en pantalla. Normalmente, yo creo una cesta diferente para cada tipo de información (Whois, medios sociales, etcétera). Después, hago un poco de trabajo de reconocimiento utilizando Google Maps

o Google Earth para capturar algunas imágenes del edificio o instalaciones del cliente, que también puedo guardar en BasKet. Cuando completo la auditoría, recuperar y utilizar la información rápidamente es muy sencillo. La figura 2.2 muestra una cesta de BasKet casi completa con mucha información útil y varias fichas.

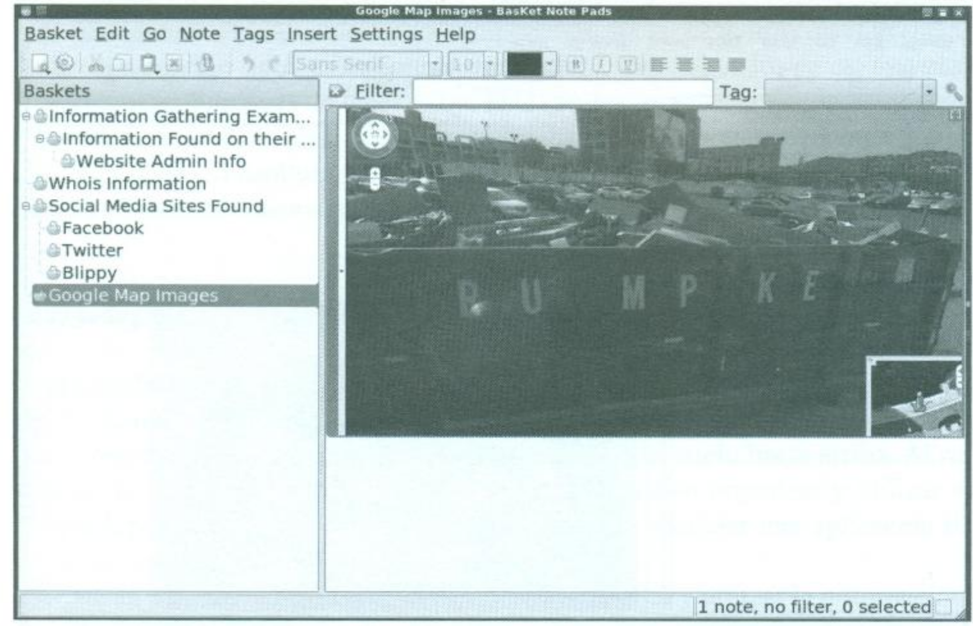


Figura 2.2. *Una cesta de BasKet casi completa con mucha información útil.*

Como muestra la figura 2.2, en BasKet es posible almacenar la información en un formato cómodo de leer. Procuro incluir toda la información que pueda porque ningún dato es demasiado pequeño para guardarse. La información que incluyo son elementos del sitio Web del cliente, información Whois, sitios de medios sociales, imágenes, datos de contacto de los empleados, historiales, foros, aficiones y todo lo que encuentre relacionado con la empresa.

Cuando termino, simplemente hago clic en el menú Basket, después hago clic en Export y exporto la cesta completa como una página HTML. Esto es estupendo para hacer informes o compartir la información.

Para un ingeniero social reunir información, como se discutirá en detalle más adelante, es la clave de cada actuación pero si no puede recuperar y utilizar la información rápidamente, entonces resulta inútil. Una herramienta como BasKet hace que guardar y utilizar los datos sea muy sencillo. Si prueba BasKet una vez, le enganchará.

La utilización de Dradis

Aunque BasKet es una gran herramienta, si hace mucha recopilación de información o si trabaja en equipo y necesita reunir, guardar y utilizar los datos, entonces es importante tener una herramienta que permita compartir la información por varios usuarios. Esa herramienta es Dradis. Según los creadores de la fuente abierta de Dradis, el programa es una "aplicación Web independiente que proporciona un almacén centralizado de la información" que se ha reunido y un medio a partir del que planificar los siguientes pasos. Al igual que BasKet, Dradis es una herramienta de software libre y de fuente abierta que puede encontrarse en `http//dradisframework.org/`. Tanto para Linux, Windows o Mac, Dradis tiene unas instrucciones de configuración e instalación sencillas que se pueden encontrar en `http://dradisframework.org/install.html`.

Una vez que Dradis está instalado y es configurado, navegue al *localhost* y el puerto que haya asignado o utilice el estándar 3004. Puede hacerlo abriendo el navegador e introduciendo `https://localhost:3004/`. Una vez iniciada la sesión, le recibe la pantalla de la figura 2.3. Fíjese en el botón Add Branch (Añadir nueva rama), arriba a la izquierda. Añadir una nueva rama le permite incluir elementos parecidos a los de BasKet: notas, imágenes, etc. Puede incluso importar notas.

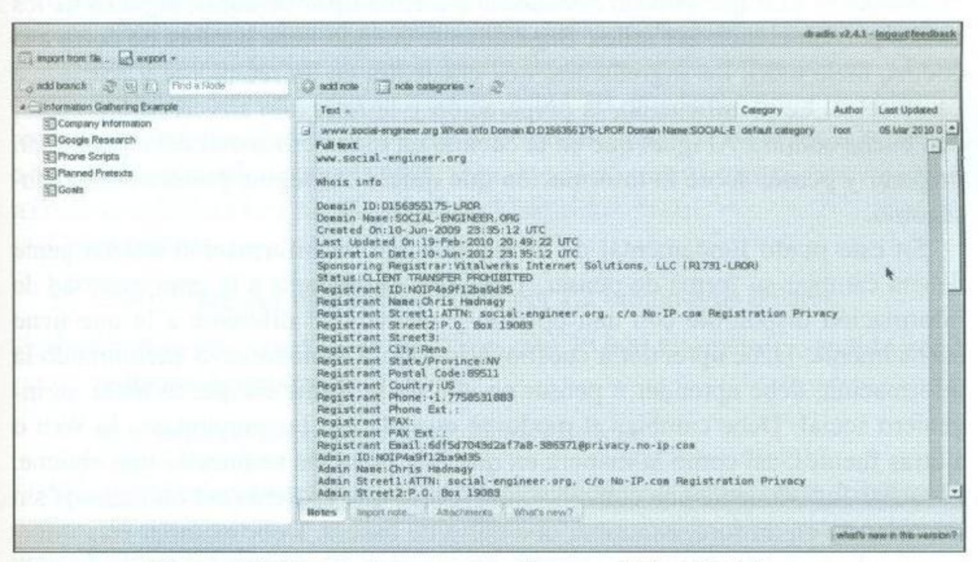


Figura 2.3. *Dradis tiene una interfaz agradable y fácil de usar.*

Dradis y BasKet son sólo dos de las herramientas que he utilizado para recopilar y guardar información. Los sitios Web de Dradis y BasKet tienen buenos tutoriales sobre la configuración y la utilización de estas potentes herramientas.

Sea cual sea el sistema operativo que utilice (Mac, Windows o Linux), tiene varias opciones donde elegir. Lo importante es utilizar una herramienta con la que esté cómodo y que pueda manejar grandes cantidades de información.

Por este motivo, le sugiero evitar productos como Notepad de Windows o Smultron o TextEdit de Mac. Necesita poder dar formato y destacar ciertas áreas de su información. En mi servidor Dradis, mostrado en la figura 2.3, tengo una sección para guiones telefónicos. Esta función es útil para transcribir ideas que pueden funcionar en base a la información reunida.

Estos instrumentos sugieren cómo empieza el ingeniero social a utilizar la información que reúne. La primera fase para utilizar los datos que recopila es pensar como un ingeniero social.

Pensar como un ingeniero social

Tener unos cuantos cientos de megabytes de información e imágenes está muy bien, pero cuando empieza a repasarla, ¿cómo se habitúa a examinar y estudiar esa información para lograr el mayor impacto?

Por supuesto, puede simplemente abrir un navegador e introducir extensas búsquedas al azar que pueden conducirle a ciertos tipos de datos, algunos de los cuales pueden incluso ser útiles. Seguramente cuando tiene hambre no corre a la cocina, mete todos los ingredientes que encuentra en un recipiente y empieza a comérselos. La planificación, la preparación y la reflexión sirven para preparar una buena comida. Al igual que en la cocina, un ingeniero social debe planificar, preparar y pensar sobre la información que quiere conseguir y sobre cómo conseguirla.

En este punto fundamental de la recopilación de información mucha gente deberá cambiar su forma de pensar. Tiene que enfrentarse a la gran cantidad de información disponible con una opinión y mentalidad diferente a la que tiene normalmente. Debe aprender a cuestionarlo todo y, cuando vaya encontrando la información, debe aprender a pensar en ella de la forma en que lo haría un ingeniero social. Debe cambiar el modo en que plantea las preguntas a la Web o a otras fuentes, así como la manera en que interpreta las respuestas que obtiene. Escuchar furtivamente una conversación, leer lo que aparenta ser un mensaje sin importancia en un foro, examinar una bolsa de basura. Debe asimilar esta información de un modo distinto a como lo hacía antes. A mi mentor Mati le encanta encontrar fallos de programa. ¿Por qué? Porque es un probador de seguridad y un escritor de *exploit*. Un fallo en un programa es el primer paso para encontrar una vulnerabilidad en el software, por lo que, en lugar de enfadarse por la pérdida de datos, se alegra por el fallo. Un ingeniero social debe tratar la información de un

modo muy semejante. Cuando encuentre un objetivo que utiliza muchos sitios Web diferentes de medios sociales, busque los vínculos entre ellos y la información con la que pueda crear un perfil completo.

Como ejemplo, en una ocasión alquilé un coche para hacer un viaje de negocios. Mi acompañante y yo cargamos nuestro equipaje en el maletero; cuando entramos en el coche reparamos en una pequeña bolsa de basura que había en el asiento de atrás. La persona que iba conmigo dijo: "Este servicio va de mal en peor. Se supone que por lo que pagamos podrían al menos limpiar el coche".

Es cierto, sería lo lógico, pero antes de que tirara la bolsa a un cubo cercano, dije: "Déjame echar un vistazo rápido". Cuando abrí la bolsa y aparté los envoltorios de unos bocadillos, lo que encontré allí a simple vista me resultó muy impactante: era la mitad de un cheque partido. Rápidamente, volqué el contenido de la bolsa y encontré un recibo de banco y la otra mitad del cheque. Era un cheque de unos dos mil dólares roto en pedazos (no en pequeños trozos, sino en cuatro grandes pedazos) que habían arrojado a una pequeña bolsa junto a los envoltorios de unos bocadillos. Una vez pegado con cinta, el cheque revelaba el nombre de la persona, el nombre de su empresa, su número de teléfono, su número de cuenta bancaria y el código de identificación bancaria. Por suerte para él, no soy una mala persona porque sólo se necesitan un par de pasos más para cometer un robo de identidad.

Esta historia personifica la relación que tiene la gente con su información valiosa. Esta persona alquiló el coche antes que yo y después, al tirar el cheque, estaba convencido de que lo había hecho desaparecer de forma segura. O eso pensó; pero éste no es un caso aislado. En esta URL puede encontrar una historia reciente sobre cosas muy valiosas que le gente simplemente ha tirado a la basura o ha vendido por prácticamente nada: `www.social-engineer.org/wiki/archives/BlogPosts/LookWhatIFound.html`.

Cosas como:

- Una pintura que un museo compró por 1,2 millones de dólares.
- Un Bugatti Type 57S de 1937 con sólo 39.000 kilómetros, vendido por 3 millones de dólares.
- Una copia de la declaración de independencia.

Si la gente tira pinturas con una copia escondida de la declaración de independencia, probablemente no le dará importancia a tirar recibos, historiales médicos, viejas facturas o extractos de la tarjeta de crédito.

El modo en el que interactúa con la gente en público puede tener efectos devastadores. En la siguiente situación, me pidieron auditar una empresa y antes de proceder tenía que reunir cierta información. Preste atención a cómo una sencilla información aparentemente insignificante puede conducir a una brecha.

Simplemente siguiendo a uno de los altos cargos de la empresa objetivo durante un par de días descubrí que paraba a tomar café en el mismo sitio todas las mañanas. Como conocía su parada de las siete y media para tomar café en la cafetería local, pude preparar un "encuentro". Él se sentaría durante 30 minutos, leería el periódico y tomaría un café con leche. Entré en la cafetería cinco minutos después de que se sentara. Pedí la misma bebida que él y me senté a su lado. Observé que dejaba a un lado una sección del periódico y le pregunté si me permitía leerla. Como había leído el periódico antes de entrar, sabía que en la página 3 había un artículo sobre un asesinato reciente en la zona. Actué como si lo acabara de leer y dije en alto: "Incluso en estas pequeñas ciudades las cosas se están poniendo peligrosas. ¿Vive usted por aquí?".

En ese momento el objetivo podía rechazarme o, si jugaba bien mis cartas, mi lenguaje corporal, el tono de mi voz y mi aspecto le relajarían. Dijo: "Sí, me mudé aquí hace unos años por un trabajo. Me gustan las ciudades pequeñas, pero cada vez se oyen más cosas de ese tipo".

Continué: "Yo estoy viajando por la zona. Vendo servicios de consultoría de gama alta para empresas y me gusta viajar por las ciudades pequeñas pero parece que cada vez oigo más historias como ésta en las zonas rurales". Entonces, en un tono casual y bromista, dije: "¿No será usted por casualidad un pez gordo de una gran empresa que necesita un servicio de consultoría, verdad?".

Se rió mucho y, entonces, como si se sintiera retado a probar su valía, dijo: "Bueno, soy vicepresidente local de finanzas de la empresa XYZ, pero no manejo ese departamento".

"Oiga, mire, no es que quiera venderle nada, le dejo disfrutar de su café, pero ¿cree que podría pasarme mañana o el miércoles a dejarle esta información?".

Entonces fue cuando la historia se puso interesante. Dijo: "Bueno, no me importaría pero el miércoles me voy de vacaciones. Unas vacaciones bien merecidas, por cierto. Pero, ¿por qué no me la envía por correo electrónico y yo le llamo?". Entonces me dio su tarjeta.

"Supongo que va a algún sitio soleado". Dije esto sabiendo que probablemente me estaba acercando al punto en el que tenía que cortar para no levantar sospechas.

"Llevo a mi mujer a un crucero por el sur". Me di cuenta de que no quería decirme dónde iba, lo cual está bien, así que nos dimos la mano y nos separamos.

¿Podía haberme evitado? Probablemente, pero ahora yo tenía una información valiosa. Sabía:

- Su número directo.
- Cuándo se iba de vacaciones.
- Qué tipo de vacaciones.

- Que era un directivo local.
- El nombre de la empresa.
- Su puesto en la empresa.
- Que se había mudado recientemente.

Por supuesto, había datos que ya conocía por la recopilación de información que había hecho previamente, pero pude añadir una buena cantidad después de este encuentro. Entonces, para iniciar la siguiente parte del ataque, llamé a su número directo el día después del que supuestamente se iba y pregunté por él. Su secretaria me dijo: "Lo siento, pero el señor Smith está de vacaciones. ¿Quiere dejarle algún mensaje?". Excelente. Se confirmaba la información y ahora lo único que tenía que hacer era poner en marcha la fase final, lo que significaba vestirme con un traje y llevar mis tarjetas de visita de 9 euros a su oficina. Entré, me registré y le dije a la secretaria que tenía una cita con el señor Smith a las 10 de la mañana. Ella contestó: "Está de vacaciones, ¿está usted seguro de que era hoy?".

Poniendo en práctica mis sesiones de microexpresión, un tema tratado en el capítulo 5, mostré verdadera sorpresa: "Un momento, ¿su crucero era esta semana? Pensaba que era la próxima". Bien, esta frase es fundamental. ¿Por qué?

Quería que la cita pareciese real y, de paso, ganarme la confianza de la secretaria. Afirmando que sabía lo del crucero, debía significar que el señor Smith y yo habíamos tenido una conversación personal (lo suficiente como para que yo supiera su itinerario). Mi impotencia provocó lástima en la secretaria, que enseguida quiso ayudarme: "Oh, vaya, lo siento, ¿quiere que llame a su ayudante?".

"Ah, no", contesté. "Necesitaba dejarle una información. Qué te parece esto, ¿te la puedo dejar a ti y se la das cuando vuelva? Estoy avergonzado. ¿Podrías no contarle lo que he hecho?".

"Mis labios están sellados".

"Gracias. Bueno, ya me voy, pero ¿puedo utilizar el servicio un momento?". Sabía que normalmente no me dejarían entrar, pero esperaba que la combinación de mis dotes comunicativas, la impotencia mostrada y su lástima pudiera tener éxito. Y lo tuvo.

En el servicio dejé un sobre en un estante y le puse una pegatina que decía PRIVADO. Dentro del sobre "privado" había una llave USB con una carga maliciosa. También dejé un sobre en un pasillo junto a una sala de descanso para aumentar las posibilidades de que alguien encontrara alguno de los dos y fuera lo suficientemente curioso para insertarlo en su ordenador.

Efectivamente, este método parece que funciona siempre. Lo más inquietante es que este ataque probablemente no hubiera funcionado de no ser por una insignificante conversación en una cafetería.

La cuestión no sólo está en cómo unos pequeños datos pueden conducir a una brecha, sino también en cómo se reúne esa información. Es importante comprender y probar las fuentes que puede utilizar para recopilar información hasta que domine cada método y cada fuente de recopilación. Hay muchos tipos diferentes de fuentes. Un buen ingeniero social debe estar preparado para pasar algún tiempo aprendiendo las fortalezas y debilidades de cada una, así como el mejor modo de utilizar cada fuente, lo que es el tema de la siguiente sección.

Fuentes de recopilación de información

Existen muchas fuentes diferentes de recopilación de información. La siguiente lista no puede abarcar todas las posibilidades existentes, pero perfila las opciones más importantes.

Recopilar información de los sitios Web

Los sitios Web personales o corporativos pueden proporcionar una gran cantidad de información. Lo primero que hará normalmente un buen ingeniero social es reunir todos los datos que pueda del sitio Web de la persona o de la empresa. Dedicarle tiempo al sitio Web puede llevarle a entender claramente:

- Lo que hacen.
- Los productos y servicios que ofrecen.
- Las localizaciones físicas.
- Las ofertas de puestos de trabajo.
- Los números de contacto.
- Las biografías de los ejecutivos o del consejo administrativo.
- El foro de apoyo.
- La nomenclatura de los correos electrónicos.
- Palabras o frases especiales que pueden ayudar a determinar contraseñas.

Navegar en los sitios Web personales de la gente también es muy interesante porque muchas veces incluyen detalles íntimos de sus vidas: niños, casas, trabajos, etc. Esta información debe catalogarse en secciones porque en ocasiones habrá algo de esta lista que puede utilizarse en el ataque.

A menudo, los empleados de la empresa formarán parte de los mismos foros, listas de correo o sitios Web de medios sociales. Si encuentra a un empleado en LinkedIn o en Facebook, hay muchas posibilidades de que algunos de sus com-

pañeros estén ahí también. Conseguir reunir toda esta información puede ayudar realmente a un ingeniero social a retratar a la empresa y a sus empleados. Muchos empleados pueden hablar de su puesto de trabajo en sus intervenciones en los medios sociales. Esto puede servir para determinar cuánta gente trabaja en un departamento y cómo está estructurado ese departamento.

Motores de búsqueda

Johnny Long escribió un famoso libro llamado *Hacking con Google* que descubrió a la gente la asombrosa cantidad de información que posee Google.

Google perdona pero nunca olvida y es comparado con "el gran oráculo". Siempre que sepa cómo preguntar, puede decirle prácticamente todo lo que quiera saber.

Johnny creó una lista de lo que él llama "Google Dorks", unas cadenas que pueden utilizarse para buscar en Google información sobre una empresa. Por ejemplo, si escribe: **site:Microsoft.com filetype:pdf**, obtendrá una lista con todos los archivos con la extensión PDF que haya en el dominio `microsoft.com`.

Estar familiarizado con los términos de búsqueda que pueden ayudarle a localizar archivos de su objetivo es un parte muy importante de la recopilación de información. Yo tengo la costumbre de hacer búsquedas como **filetype:pdf**, **filetype:doc**, **filetype:xls** y **filetype:txt**. También es buena idea comprobar si los empleados dejan abiertos en sus servidores archivos como DAT, CFG u otros archivos de bases de datos o configuración. Hay libros enteros dedicados al tema de utilizar Google para encontrar información, pero lo más importante que hay que recordar es que aprender los operandos de Google le ayudará a desarrollar los suyos propios.

Un sitio Web como `www.googleguide.com/advanced_operators.html` tiene una buena lista de los operandos y explica cómo utilizarlos.

Google no es el único motor de búsqueda que revela información asombrosa. Un investigador llamado John Matherly creó un motor de búsqueda llamado Shodan (`www.shodanhq.com`). Shodan es único en cuanto a que busca en la red servidores, *routers*, software específico y mucho más. Por ejemplo, una búsqueda de **microsoft-iis os:"Windows 2003"** revela las siguientes cantidades de servidores que utilizan Windows 2003 con Microsoft IIS:

- Estados Unidos 59.140.
- China 5.361.
- Canadá 4.424.
- Reino Unido 3.406.
- Taiwán 3.027.

Esta información no es relevante en relación a un objetivo concreto pero demuestra una lección fundamental: la red contiene una cantidad increíble de datos que deben ser explotados por un ingeniero social que pretenda dominar la recopilación de información.

Reconocimiento de Whois

Whois es el nombre de un servicio y una base de datos. Las bases de datos de Whois contienen gran cantidad de información y en algunos casos pueden incluso contener datos de contacto completos de los administradores del sitio Web.

Utilizar una línea de comando de Linux o un sitio Web como `www.whois.net` puede conducirle a resultados sorprendentemente específicos tales como la dirección de correo electrónico de una persona, el número de teléfono o incluso la dirección IP del servidor DNS.

La información de Whois puede ser muy útil para perfilar una empresa y descubrir detalles sobre sus servidores.

Todos estos datos pueden utilizarse para nuevas recopilaciones de información o para lanzar ataques de ingeniería social.

Servidores públicos

Los servidores públicos de una empresa también son buenas fuentes de la información que sus sitios Web no proporcionan. Tomar las huellas a un servidor para determinar sus OS, las aplicaciones instaladas y la información de IP pueden proporcionar mucha información sobre la infraestructura de una empresa. Una vez determinada la plataforma y las aplicaciones en uso, puede combinar esta información con una búsqueda en el nombre de dominio corporativo para encontrar entradas en foros públicos.

Las direcciones de IP pueden decirle si los servidores están alojados localmente o con un proveedor; con los registros de DNS puede determinar nombres y funciones de servidores y direcciones IP.

En una auditoría, después de buscar en la red utilizando una herramienta llamada Maltego (explicada en el capítulo 7), conseguí sacar a la luz un servidor público que contenía literalmente cientos de documentos con información clave de proyectos, clientes y de los creadores de esos proyectos. Esta información fue devastadora para la empresa.

Un apunte importante a tener en cuenta es que realizar un rastreo de puerto (utilizando una herramienta como NMAP u otro rastreador para localizar puertos abiertos, software y sistemas operativos utilizados en un servidor público) puede acarrear problemas con la ley en algunos lugares.

Por ejemplo, en junio de 2003 un israelí llamado Avi Mizrahi fue acusado por la policía israelí del delito de intento de acceso no autorizado a material informático. Había realizado un rastreo de puerto del sitio Web del Mossad (el servicio secreto israelí). Unos ocho meses después, fue absuelto de todos los cargos. El juez incluso dictaminó que este tipo de acciones no deben ser desalentadas cuando se realizan en un sentido positivo (`www.law.co.il/media/computer-law/mizrachi_en.pdf`).

En diciembre de 1999, Scout Moulton fue arrestado por el FBI y acusado de intento de acceso informático bajo la ley de protección de sistemas informáticos de Georgia y la ley nacional de abuso y fraude informático. En aquel momento, su empresa de servicios de tecnologías de la información tenía un contrato en vigor con el condado Cherokee de Georgia para mantener y mejorar la seguridad del centro de llamadas de emergencia (`www.securityfocus.com/news/126`).

Como parte de su trabajo, Moulton realizó varios rastreos de puerto en los servidores del condado Cherokee para comprobar su seguridad y finalmente rastreó un servidor Web controlado por otra empresa de tecnologías de la información. Esto provocó un pleito, aunque Moulton fue absuelto en 2000. El juez dictaminó que no se habían producido daños que perjudicaran la integridad y disponibilidad de la red.

En 2007 y 2008, Inglaterra, Francia y Alemania publicaron leyes que ilegalizan la creación, distribución y posesión de materiales que permitan a alguien violar una ley informática. Los rastreos de puertos entran en esta definición.

Por supuesto, si va a realizar una auditoría profesional a una empresa, estos detalles se aclaran en el contrato, pero es importante señalar que es responsabilidad del auditor conocer las leyes locales y asegurarse de no violarlas.

Medios sociales

Muchas empresas han empezado a interesarse por los medios sociales. Es publicidad barata que llega a un gran número de clientes potenciales. También es una nueva corriente de información de una empresa que puede proporcionar algunos datos útiles. Las empresas publican noticias sobre eventos, nuevos productos, notas de prensa e historias que pueden relacionarlas con eventos de actualidad.

Últimamente, las redes sociales han desarrollado un modo de proceder particular. Da la sensación de que cuando alguna tiene éxito aparecen unas cuantas más que utilizan una tecnología parecida. Con sitios como Twitter, Blippy, PleaseRobMe, ICanStalkU, Facebook, LinkedIn, MySpace y otros, puede encontrar fácilmente información sobre la vida y paradero de la gente. Más adelante, este libro trata este tema en profundidad. Verá que las redes sociales son una increíble fuente de información.

Sitios de usuarios, blogs y otros

Los sitios de usuarios como los *blogs*, wikis y vídeos *on-line* no sólo pueden proporcionar información sobre la empresa objetivo, también ofrecen una conexión más personal a través del contenido subido por el usuario. Un empleado descontento que está hablando en su *blog* sobre sus problemas en la empresa puede ser susceptible de compartir información con un lector comprensivo con las mismas opiniones y problemas. De cualquier manera, los usuarios cuelgan en la Web increíbles cantidades de información que cualquiera puede ver y leer. Aquí tiene un buen ejemplo: eche un vistazo a esta nueva Web recién aparecida: `www.icanstalku.com` (véase la figura 2.4). Al contrario de lo que indica su nombre ("puedo acosarte"), no anima a la gente a acosar a otros. Este sitio pone de manifiesto el total descuido de muchos usuarios de Twitter. Rastrea el sitio de Twitter y busca usuarios que son tan imprudentes como para colgar fotos hechas con sus teléfonos *smartphone*. Mucha gente no sabe que la mayoría de teléfonos *smartphone* incrusta datos de localización GPS en sus fotos. Cuando un usuario cuelga una foto en la Web con esta información incrustada, puede conducir a una persona hasta su localización.

Mostrar información sobre la localización es un aspecto de los sitios Web de los medios sociales. No sólo le permiten colgar fotos de sí mismo, también revelan implícitamente dónde está, posiblemente sin su conocimiento.

Sitios como ICanStalkU subrayan el peligro de esta información. Lea esta historia (una entre tantas) que muestra cómo se utilizan estos datos para robos en casas y otros delitos: `www.social-engineer.org/wiki/archives/BlogPosts/TwitterHomeRobbery.html`.

Este tipo de información puede proporcionarle un perfil muy detallado de su objetivo. A la gente le encanta *twitear* sobre dónde está, lo que está haciendo y con quién está. Blippy permite a una persona conectar sus cuentas bancarias y, básicamente, *twitea* información sobre cada compra, dónde se realizó y cuánto ha costado. Con fotos con información de localización incrustada y sitios como Facebook, que mucha gente utiliza para colgar fotos personales, historias y otra información relacionada, se cumple el sueño de cualquier ingeniero social. En un momento, se puede crear un perfil completo con la dirección de una persona, su trabajo, sus fotos, aficiones y mucho más. Otro aspecto de los sitios de los medios sociales que los hace excelentes fuentes de recopilación de información es la posibilidad de mantener el anonimato. Si el objetivo es un hombre de mediana edad recientemente divorciado al que le encanta su página de Facebook, usted puede ser una mujer joven en busca de un nuevo amigo. Cuando la gente flirtea, muchas veces divulga información muy valiosa. Combine la habilidad para ser quien quiera en la Web con el hecho de que la mayoría de la gente cree a pies juntillas todo lo que lee y lo que obtiene es uno de los riesgos más grandes para la seguridad.



Figura 2.4. *Una escena típica en la página de inicio de ICanStalkU.com.*

Informes públicos

La información pública puede ser generada por entidades dentro o fuera de la empresa objetivo. Esta información puede consistir en informes trimestrales, informes gubernamentales, informes analíticos, beneficios de empresas que cotizan en bolsa, etc. Un ejemplo son los informes de Dunn y Bradstreet u otros informes de ventas que se venden por muy poco dinero y contienen mucha información detallada de la empresa objetivo.

Otra vía analizada en más detalle más adelante es utilizar la investigación de antecedentes como los que se encuentran en `www.USSearch.com` y `www.intelius.com`. Éstos y muchos otros sitios ofrecen servicios de comprobación de antecedentes por tan sólo 1 euro por un informe limitado, hasta la posibilidad de pagar una cuota de 49 euros al mes que le permite obtener todos los informes que quiera. Puede conseguir mucha de esta información gratis

utilizando los motores de búsqueda pero algunos datos financieros detallados y datos personales sólo pueden obtenerse de forma sencilla y legal a través de un servicio de pago. Quizá lo más asombroso es que muchas de estas empresas pueden incluso proporcionar datos como el número de la seguridad social de una persona a algunos clientes.

Utilizar el poder de la observación

Aunque no se utiliza mucho como herramienta de ingeniería social, la simple observación puede aportarle mucha información sobre su objetivo. ¿Los empleados del objetivo utilizan llaves, tarjetas RFID u otros métodos para entrar en el edificio? ¿Existe un área designada para fumadores? ¿Están localizados los contenedores? ¿El edificio tiene cámaras externas? Muchas veces los elementos externos como los suministros de energía o las unidades de aire acondicionado revelan información sobre cuál es la empresa proveedora y eso puede proporcionar al ingeniero social otra vía para conseguir acceder.

Éstas son sólo algunas preguntas para las que puede conseguir respuestas a través de la observación. Tomarse algún tiempo para observar al objetivo, grabar utilizando una cámara oculta y después estudiar y analizar la información, puede enseñarle mucho y proporcionar a su archivo un gran empuje.

Mirar en la basura

Sí, por muy duro que sea imaginar pasar un rato saltando entre la basura, esta acción puede rendir algunos de los beneficios más lucrativos de la recopilación de información. A menudo, la gente tira facturas, notas, cartas, discos compactos, ordenadores, llaves USB y una gran cantidad de artilugios e informes que realmente pueden proporcionar increíbles cantidades de datos. Como señalamos previamente, si la gente tira obras de arte que valen millones de euros, entonces otras cosas que ven como desperdicios a menudo irán sin pensarlo a la basura.

En ocasiones, las empresas trituran documentos que consideran demasiado importantes para tirarlos sin más pero utilizan un triturador ineficiente que deja papeles que pueden recomponerse, como muestra la figura 2.5.

Esta imagen muestra algunos documentos después de ser triturados pero aún se pueden distinguir palabras completas. Este tipo de trituración puede desbaratarse con un poco de tiempo y paciencia y un poco de cinta adhesiva, como muestra la figura 2.6. Los documentos que pueden recomponerse, aunque sea parcialmente, pueden revelar información realmente devastadora.



Figura 2.5. *Los jirones largos permiten que aún se pueda leer algunas palabras.*

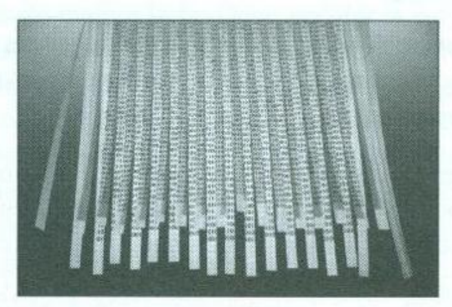


Figura 2.6. *Recomponer documentos sólo es cuestión de tiempo y paciencia.*

Sin embargo, utilizar un triturador que tritura en ambas direcciones y que deja un revoltijo picado de papel, hace que la recomposición de documentos sea prácticamente imposible, como muestra la figura 2.7.

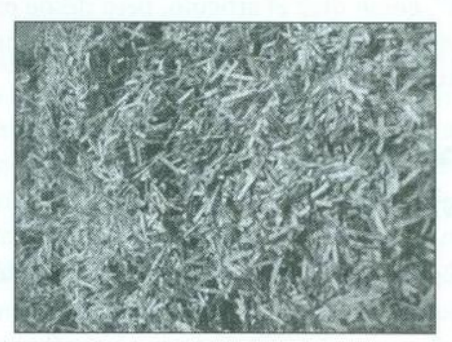


Figura 2.7. *Resulta imposible adivinar que esto antes era dinero.*

Muchas empresas utilizan servicios comerciales que se llevan sus documentos triturados para incinerarlos. Algunas empresas incluso dan sus documentos a terceros lo que, como probablemente habrá adivinado, deja abierto otro vector de ataque. Un ingeniero social que averigüe el nombre de la empresa que proporciona este servicio puede fácilmente hacerse pasar por la persona que va a recoger la do-

cumentación y quedarse con ella. En cualquier caso, inspeccionar los contenedores ofrece una forma rápida de encontrar toda la información que quiere. Recuerde algunos puntos clave cuando inspeccione contenedores:

- **Lleve puestos unos buenos zapatos o botas:** Nada puede ser más desastroso que saltar a un contenedor y que un clavo le atraviese el pie. Asegúrese de llevar un calzado que se ajuste bien y que le proteja de objetos afilados.
- **Lleve ropa oscura:** No hace falta explicar mucho. Lo mejor es ropa que no le importe que se rompa y que sea oscura para evitar que le descubran.
- **Lleve una linterna.**
- **Coja algo y corra:** A no ser que esté en un lugar tan apartado que sea imposible que le descubran, lo mejor es coger un par de bolsas e irse a otro sitio a hurgar en ellas.

Rebuscar en contenedores casi siempre conduce a información muy útil. A veces el ingeniero social ni siquiera tiene que meterse en un contenedor para encontrar lo que busca. Ya hemos mencionado este artículo en el capítulo 1 (`www.social-engineer.org/resources/book/TopScretStolen.htm`) que confirma esta idea. La unidad antiterrorista de Canadá tenía un plan para un nuevo edificio en el que se mostraban los detalles de las cámaras de seguridad, vallas y otros elementos de alto secreto. Estos planos se tiraron. Sí, se tiraron a la basura sin siquiera triturarlos y, afortunadamente, los encontró una persona con buenas intenciones. Ésta es sólo una de tantas historias que muestran el "grado al que llega la estupidez", como dice el artículo, pero desde el punto de vista de un ingeniero social, rebuscar en la basura es una de las herramientas de recopilación de información más útiles que existen.

Utilizar software de predicción de contraseñas

El capítulo 7 examina las herramientas que forman el equipo profesional de los ingenieros sociales, pero esta sección ofrece una visión general. Los sistemas de predicción de contraseñas como CUPP (*Common User Password Profiler*) y WYD (*Who's Your Daddy*) pueden ayudar a perfilar las contraseñas potenciales de una empresa o una persona. Se explica cómo utilizar estas herramientas. Lo que hace un sistema como WYD es barrer un sitio Web y crear una lista de contraseñas a partir de las palabras mencionadas en ese sitio Web. No es infrecuente que la gente utilice palabras, nombres o fechas como contraseñas. Este tipo de software consigue fácilmente crear listas para probar combinaciones.

Herramientas increíbles como Maltego (vea el capítulo 7 para más detalles), creado por Paterva, son el sueño del recopilador de información. Maltego permite al ingeniero social realizar muchas búsquedas pasivas en la red, sin tener que utilizar nada más que el propio Maltego. Después, guarda esta información y la expresa en gráficos en pantalla para que pueda utilizarse para elaborar informes, para exportar o para otros propósitos. Esto puede ayudar mucho en la elaboración del perfil de una empresa.

Recuerde: su meta cuando recopila datos es informarse sobre la empresa objetivo y sobre las personas que forman parte de la empresa. Una vez que el ingeniero social ha reunido suficiente información, en su mente se forma una imagen clara de las mejores formas de manipularla. Debe perfilar la empresa como un todo y descubrir en la medida de lo posible cuántos empleados forman parte de algún club o grupo o tienen ciertas aficiones. ¿Hacen donaciones a alguna obra social? ¿Sus hijos van al mismo colegio? Toda esta información es muy útil para desarrollar un perfil. Un perfil claro puede ayudar al ingeniero social no sólo a desarrollar un buen pretexto, sino también a reconocer qué preguntas hacer, qué días son buenos o malos para llamar o presentarse en el lugar, así como muchas otras pistas que pueden hacer mucho más fácil el trabajo.

Todos los métodos explicados hasta ahora son sobre todo físicos, métodos muy personales de recopilación de información. No he tocado la parte más técnica de la recopilación de información, servicios como SMTP, DNS, Netbios y el poderoso SNMP. En el capítulo 7 explico con más detalle algunos de los aspectos más técnicos con los que Maltego puede ayudar. Merece la pena examinar estos métodos pero tienen una naturaleza mucho más técnica en oposición a los métodos más "humanos".

Sea cual sea el modo que utilice para reunir información de forma lógica, la pregunta que puede surgir es: ahora que sabe dónde acudir para recopilar datos, ¿cómo hacerlo? ¿Cómo catalogar la información, cómo guardarla y presentarla? ¿Qué puede hacer con ella? Como ingeniero social, una vez que tiene la información, debe empezar a planear los ataques. Para hacerlo, debe empezar desarrollando un plan que utilice estos datos. Una de las mejores maneras para empezar a utilizar esta información es desarrollar lo que se llama un modelo de comunicación.

Desarrollar un modelo de comunicación

Cuanto más elaboradas son muestras formas de comunicación, menos comunicamos.
Joseph Priestley

La "comunicación" es el proceso de transferir información de una entidad a otra. Implica interacciones entre, al menos, dos agentes y puede ser entendida como un proceso de doble dirección en el que hay un intercambio de información y una progresión de pensamientos, sentimientos o ideas que se dirigen hacia una meta o dirección mutuamente aceptada.

Este concepto es muy parecido a la definición de la ingeniería social, excepto en que quienes están implicados en un proceso de comunicación ya tienen una meta común, mientras que la meta del ingeniero social es utilizar la comunicación para crear una meta común. La comunicación es un proceso por el que la información es empaquetada, canalizada y transmitida por parte de un emisor hacia un receptor a través de algún medio. El receptor descodifica el mensaje y retroalimenta al emisor. Todas las formas de comunicación requieren un emisor, un mensaje y un receptor.

Como ingeniero social, es fundamental entender cómo funciona la comunicación para desarrollar un modelo adecuado. Crear un modelo ayuda al ingeniero social a decidir el mejor método de envío, el mejor método de retroalimentación y el mejor mensaje a utilizar.

La comunicación puede presentar muchas formas diferentes. Hay métodos auditivos, como los discursos, las canciones o el tono de voz y hay métodos no verbales, como el lenguaje corporal, el lenguaje de signos, el paralenguaje, el tacto o el contacto visual. Independientemente del tipo utilizado, el mensaje y la forma de envío tendrán un efecto definitivo en el receptor.

Entender las reglas básicas es fundamental para construir un modelo para un objetivo. Algunas reglas no se pueden violar como el hecho de que la comunicación siempre tiene un emisor y un receptor. También debe tenerse en cuenta que todo el mundo tiene realidades personales diferentes que se construyen y se ven afectadas por sus experiencias pasadas y por sus percepciones.

Todo el mundo percibe, experimenta e interpreta las cosas de manera distinta en base a estas realidades personales. Cualquier evento será siempre percibido de manera diferente por gente distinta debido a este hecho. Si tiene hermanos, un buen ejercicio para confirmarlo es preguntarles su interpretación o recuerdo de un evento, especialmente si es un evento emotivo. Comprobará que su interpretación de ese evento es muy diferente a lo que usted recordaba. Cada persona tiene un espacio personal físico y mental y, dependiendo de muchos factores, permite o no a otras personas entrar en ese espacio. Cuando se comunica de cualquier forma con alguien, está intentando entrar en su espacio personal. Cuando un ingeniero social se comunica, está intentando traer a otra persona a su espacio y compartir su realidad personal. La comunicación efectiva intenta llevar a todos los participantes al espacio mental de todos los demás. Esto sucede en todas las interacciones, pero es tan habitual que la gente lo hace sin pensar en ello.

En las comunicaciones interpersonales se envían dos capas de mensajes: la verbal y la no verbal. La comunicación normalmente contiene una parte verbal o lingüística, ya sea palabra hablada o escrita. También suele tener una parte no verbal: las expresiones faciales, el lenguaje corporal o algunos mensajes no lingüísticos como los "emoticonos" o el tipo de fuente. Independientemente de la cantidad de cada uno de los tipos (verbal o no verbal), este paquete de comunicación se envía al receptor y se filtra a través de su realidad personal. El receptor formará un concepto basado en su realidad y después empezará a interpretar el paquete. Al descifrar el mensaje, el receptor va interpretándolo, incluso aunque esa interpretación no sea la que el emisor pretendía. El emisor sabrá si el paquete ha sido recibido como pretendía si el receptor devuelve un paquete de comunicación indicando su aceptación o rechazo del paquete original.

Aquí el paquete es la forma de comunicación: las palabras o letras o correos electrónicos enviados. Cuando el receptor recibe el mensaje, tiene que descifrarlo. La interpretación que haga depende de muchos factores. Si está de buen humor, de mal humor, alegre, triste, enfadado o si se siente compasivo; todo esto, además del resto de elementos que alteran su percepción, le ayuda a descifrar el mensaje. La meta del ingeniero social debe ser darle a los elementos verbales y no verbales el poder de alterar la percepción del objetivo para lograr el impacto que se desea. Éstas son algunas otras reglas básicas de la comunicación:

- Nunca dé por sentado que la realidad del receptor es igual a la suya.
- Nunca dé por sentado que el receptor va a interpretar el mensaje como se pretendía.
- La comunicación no es algo absoluto o limitado.
- Entienda siempre que hay tantas realidades diferentes como personas hay implicadas en la comunicación.

Conocer estar reglas puede mejorar la habilidad para una comunicación buena y útil. Todo esto está muy bien pero, ¿qué tiene que ver la comunicación con desarrollar un modelo? Aún más, ¿qué tiene que ver con la ingeniería social?

El modelo de comunicación y sus raíces

Como ya se ha explicado, la comunicación consiste básicamente en enviar un paquete de información a un receptor concreto. El mensaje puede proceder de diversas fuentes como la vista, el sonido, el tacto, el olfato y las palabras. Este paquete es procesado después por el objetivo y utilizado para formar una imagen general sobre "lo que se ha dicho".

Este método de valoración se llama "el proceso de comunicación". Fue establecido originalmente en 1947 por los científicos sociales Claude Shannon y Warren Weaver, cuando desarrollaron el modelo Shannon-Weaver, conocido también como "el padre de todos los modelos".

Según la Wikipedia, el modelo Shannon-Weaver "encarna los conceptos de fuente de información, mensaje, transmisor, señal, canal, ruido, receptor, destino de la información, probabilidad de error, codificación, descodificación, velocidad de la información [y] capacidad del canal", entre otras cosas.

Shannon y Weaver definieron este modelo con un gráfico, como muestra la figura 2.8.

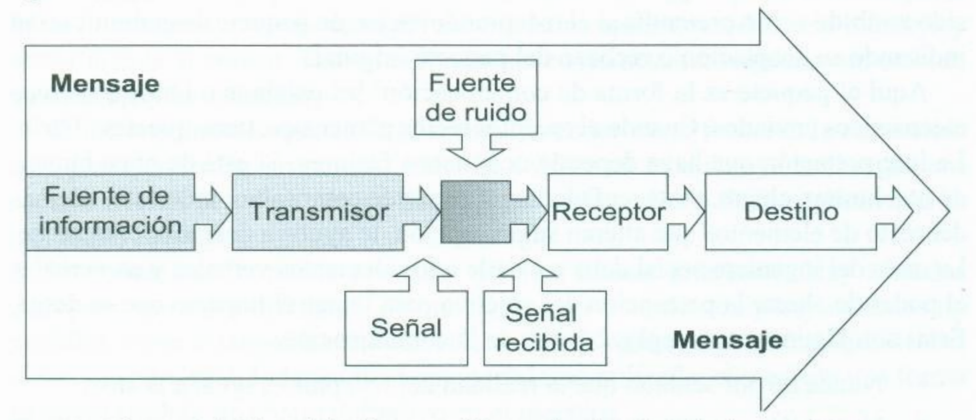


Figura 2.8. *El modelo Shannon-Weaver, "padre de todos los modelos".*

En un modelo sencillo, conocido como modelo de transmisión, la información o el contenido se envía en alguna forma de un emisor a un destino o receptor. Este concepto común de comunicación simplemente la ve como un medio para enviar y recibir información. Las fortalezas de este modelo residen en su simplicidad, generalidad y su carácter cuantificable. Shannon y Weaver estructuraron este modelo en base a:

- Una fuente de información, que produce un mensaje.
- Un transmisor, que codifica el mensaje en señales.
- Un canal, por el que las señales se adaptan para la transmisión.
- Un receptor, que "descodifica" (reconstruye) el mensaje de la señal.
- Un destino, donde llega el mensaje.

Argumentaron que existen tres niveles de problemas para la comunicación en esta teoría:

- **El problema técnico:** ¿Con qué exactitud se puede transmitir el mensaje?
- **El problema semántico:** ¿Con qué precisión se transmite el significado?
- **El problema de la efectividad:** ¿Con qué efectividad el mensaje recibido afecta a la conducta? Es importante recordar este último punto. La meta absoluta del ingeniero social es crear la conducta que se desea.

Casi 15 años más tarde, David Berlo expandió el modelo lineal de Shannon y Weaver y creó el modelo de comunicación Emisor-Mensaje-Canal-Receptor (EMCR). EMCR separa el modelo en partes distinguibles (véase la figura 2.9).

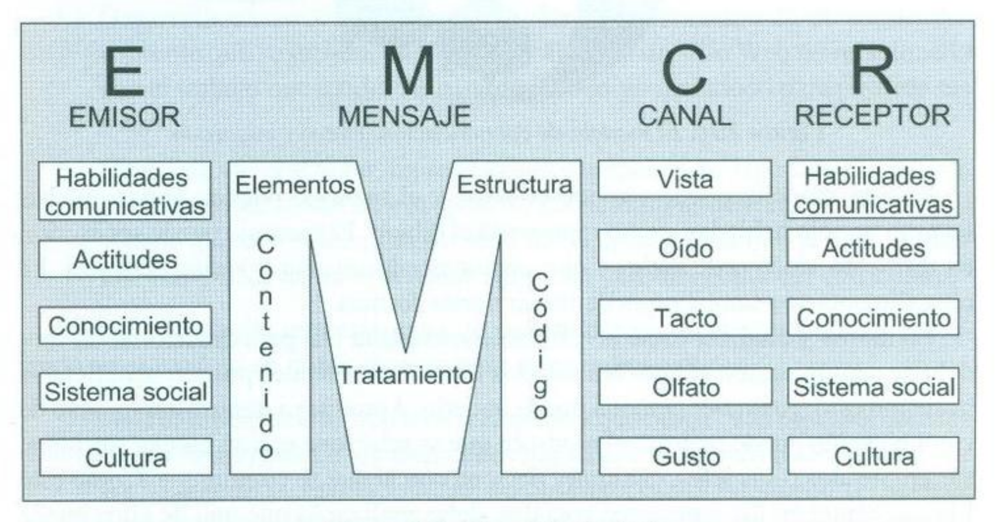


Figura 2.9. *El modelo de Berlo.*

Puede pensar en la comunicación como los procesos de transmisión de información gobernados por tres niveles de reglas:

- Propiedades formales de los signos y los símbolos.
- Las relaciones entre los signos/expresiones y sus usuarios.
- Las relaciones entre los signos y los símbolos y lo que representan.

Por lo tanto, en adelante puede precisar la definición de comunicación como la interacción social en la que al menos dos agentes comparten un grupo de signos común y un grupo de reglas comunes.

En 2008, otro investigador, D.C. Barnlund, combinó la investigación de muchos de sus predecesores con la suya y desarrolló el modelo de comunicación transaccional, mostrado en la figura 2.10.

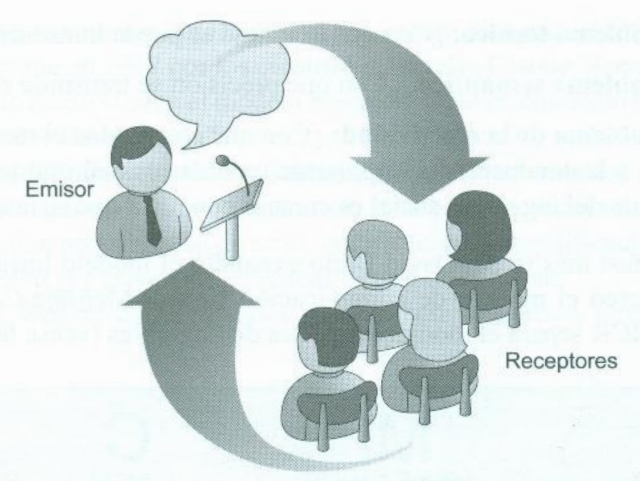


Figura 2.10. El modelo de comunicación, nuevo y mejorado.

En este modelo, puede ver que el canal y el mensaje pueden tomar muchas formas, no sólo habladas, como representa el dibujo. El mensaje puede ser escrito, en forma de vídeo o de audio y el receptor puede ser una o varias personas. La retroalimentación también puede tomar varias formas.

Combinar y analizar estas investigaciones resulta útil para desarrollar un modelo de comunicación sólido. No sólo los ingenieros sociales pueden beneficiarse haciendo esto, cualquier persona puede hacerlo. Aprender a desarrollar un plan de comunicación puede mejorar el modo en que se relaciona con su pareja, sus hijos, sus empleados o sus jefes, cualquier persona con la que se comunique. Como este libro se centra en los ingenieros sociales, debe analizar lo que uno de ellos puede aprovechar de todo esto. Después de leer toda esta teoría, puede empezar a preguntarse cómo puede utilizarse. Recuerde: un ingeniero social debe ser un maestro de la comunicación. Debe ser capaz de entrar y permanecer en el espacio mental y personal de una persona y no ofenderla ni hacer que desconecte. La llave para lograr esta meta es desarrollar, implementar y practicar modelos de comunicación efectivos. Por lo tanto, el siguiente paso es desarrollar un modelo.

Desarrollar un modelo de comunicación

Ahora que conoce los elementos fundamentales de un modelo de comunicación, examínelos desde el punto de vista de un ingeniero social:

- **La fuente:** El ingeniero social es la fuente de la información o comunicación que se va a transmitir.
- **El canal:** Es la forma de envío.

- **El mensaje:** Probablemente, la parte más importante del mensaje es saber qué le va a decir al receptor o receptores.
- **El receptor o receptores:** Éste es el objetivo.
- **La retroalimentación:** ¿Qué quiere que hagan después de transmitirles correctamente la comunicación?

¿Cómo puede utilizar estos elementos de forma efectiva? El primer paso es establecer su meta. Pruebe a trabajar con dos de los escenarios que pueden ser parte de una actuación típica de ingeniería social:

- Desarrolle un correo electrónico de *phishing* destinado a 25-50 empleados e intente que se dirijan, en horas de trabajo, a un sitio Web no relacionado con el trabajo que tendrá incrustado un código malicioso para piratear sus redes.
- Haga una visita al lugar, representando el papel de un aspirante a un puesto de trabajo que acaba de estropear su currículum al derramar café sobre él y tiene que convencer a la persona de recepción para que le deje insertar una llave USB en un ordenador para imprimir una copia del currículum.

Cuando desarrolle una estrategia de comunicación, puede encontrarse trabajando en el modelo en orden inverso para que sea provechoso.

- **Retroalimentación:** ¿Cuál es la respuesta que busca? La respuesta deseada es que la mayoría de los empleados hagan clic en el correo electrónico que les ha mandado. Eso es lo ideal; no obstante, estará satisfecho si consigue a un puñado o incluso a uno solo, pero la meta, la respuesta deseada, es que la mayoría de los objetivos hagan clic en el vínculo de *phishing*.
- **Receptores:** Aquí es donde le vienen bien sus habilidades para la recopilación de información. Tiene que saberlo todo sobre sus objetivos. ¿Les gustan los deportes? ¿Son mayoritariamente hombres o mujeres? ¿Son miembros de algún club local? ¿Qué hacen en su tiempo libre? ¿Tienen familias? ¿Son jóvenes o mayores? La respuesta a estas preguntas ayudará al ingeniero social a elegir el mensaje que va a enviar.
- **Mensaje:** Si el objetivo son hombres, mayoritariamente entre 25 y 40 años, algunos de ellos participantes de ligas fantásticas de fútbol o baloncesto, sus objetivos harán clic en vínculos sobre deportes, mujeres o un evento deportivo. Es fundamental desarrollar el contenido del correo electrónico, pero también es importante tener en cuenta la gramática, la ortografía y la puntuación. Muchos de los correos electrónicos de *phishing* se han descubierto en el pasado debido a la mala ortografía.

Un correo electrónico en el que ponga algo así: "Clikea akí y introduce tu contraseña xa verificar tu estado de cuenta", se está delatando a sí mismo. Su correo electrónico debe ser legítimo, con una buena ortografía y una oferta atractiva que encaje con el objetivo. Incluso con la misma meta, el mensaje cambiará dependiendo del género, edad y muchos otros factores. El mismo correo electrónico fallaría probablemente si el objetivo fueran mayoritariamente mujeres.

- **Canal:** Identificar este elemento es fácil porque ya sabe que va a ser un correo electrónico.
- **Fuente:** De nuevo, con este elemento no hay duda, porque usted, el ingeniero social, es la fuente. Lo creíble que resulte dependerá de sus habilidades.

Escenario 1: Phishing por correo electrónico

El objetivo son 45 hombres entre las edades de 25 y 45 años. 24 de ellos participan en la misma liga fantástica de baloncesto. Entran a diario en un sitio Web (`www.myfantasybasketballeague.com`) para hacer su selección. Esto puede verificarse por las entradas en el foro.

La meta es conducirles a un sitio Web que usted ha creado y está disponible, `www.myfantasybasketballeague.com`, que está ligeramente mal escrito respecto al sitio Web real. Este sitio es un clon del sitio Web que ellos visitan, pero con un cambio: contiene un *iframe* o marco incorporado. Habrá un botón de acceso en el centro de la página y, cuando hagan clic sobre él, les llevará al verdadero sitio Web. El tiempo que tarde en hacer clic y cargarse lo aprovechará el código para piratear sus sistemas. ¿Qué escribirá en el correo electrónico? Aquí tiene una muestra que le propongo:

Hola,

Tenemos noticias estupendas en My Basket Ball League (Mi liga fantástica de baloncesto). Hemos creado nuevas herramientas que te permitirán tener más control sobre tus selecciones y también otros productos especiales. Estamos trabajando para poder ofrecer estas novedades a todos nuestros socios, pero, inevitablemente, tendrán que aplicarse tarifas especiales por el servicio.

Queremos anunciar que las primeras 100 personas que accedan conseguirán este nuevo servicio gratis. Haga clic en `este vínculo`*, después haga clic en el botón de ACCESO de la página y acceda a la Web para incorporar gratis estos servicios en su cuenta.* `www.myfantasybasketballeague.com`

Gracias

El equipo de MFBB"

Lo más probable es que este correo interese lo suficiente, al menos a los 24 que participan en esa liga, para hacer clic en el vínculo y probar esos nuevos servicios gratis. Analice el correo electrónico. Primero, contiene una oferta que resultará atractiva para los miembros de la liga. Muchos verán que es una oferta limitada a los 100 primeros, por lo que harán clic en cuanto vean el correo que será seguramente mientras estén en el trabajo. El sitio Web al que les conduce el vínculo tiene el código malicioso y, aunque la mayoría caerá en la trampa, a un ingeniero social malicioso le basta con una víctima. Observe también que el correo está bien redactado, tiene un gancho atractivo y genera la motivación suficiente para hacer clic enseguida. Es un correo electrónico perfecto basado en un modelo de comunicación sólido.

Escenario 2: La llave USB

Un escenario in situ es más difícil porque hay que llevarlo a cabo en persona. Tiene que interpretar un papel y tiene que conocer de memoria todos los detalles porque no podrá detenerse a repasar sus apuntes una vez que haya empezado. También es importante recordar que a menudo sólo hay una oportunidad para formar una impresión en los demás. Si se hace mal, se puede echar a perder el resto del trabajo.

- **Retroalimentación:** La meta en esta situación es lograr que la recepcionista acepte su llave USB que contiene un programa malicioso. El programa se cargará y barrerá su sistema en busca de información como nombres de usuario, contraseñas, cuentas de correo electrónico o archivos SAM que contienen todas las contraseñas del sistema, copiando todos estos datos en un directorio de la llave USB. También crea una conexión inversa desde el ordenador de la recepcionista a su servidor, dándole acceso a su ordenador y a la red. A mí me gusta utilizar el Metasploit Framework o el SET (*Social Engineering Toolkit*) que se relaciona con Metasploit. Metasploit ejecuta código de explotación en sus víctimas y contiene un programa incorporado llamado Meterpreter. El usuario puede copiar elementos como *keylogging*, capturas de pantalla y reconocimientos del ordenador de la víctima.
- **Receptores:** Tener un objetivo concreto puede ser complicado porque si éste muestra rechazo, el plan se estropea. Tiene que ser cálido, amigable y convincente. Tiene que actuar rápido, porque si pasa demasiado tiempo puede surgir la duda. Pero si se mueve demasiado rápido también puede generar dudas y miedo, perdiendo la oportunidad. Debe lograrse un equilibrio perfecto.
- **Mensaje:** Como está entregando el mensaje en persona, éste debe ser claro y conciso. La historia típica es que vio un anuncio en el periódico para un puesto de administrador de bases de datos y ha llamado y hablado con

Debbie, la encargada de recursos humanos. Dijo que hoy estaba ocupada pero que se podía acercar a dejar el currículum para que ella lo revise y tener una cita al final de la semana. Mientras conducía hacia allí, se le cruzó una ardilla que le hizo dar un frenazo que derramó el café por toda la mochila destrozando su currículum, entre otras cosas. En cualquier caso, ahora tiene otra cita pero le interesa mucho este trabajo y querría saber si le permitiría imprimir una nueva copia del currículum desde la llave USB.

- **Canal:** Acude en persona utilizando la comunicación verbal, facial y el lenguaje corporal.
- **Fuente:** De nuevo es usted, a no ser que tenga una buena razón para tener un sustituto.

Aparecer ante la víctima con una carpeta empapada de café puede ayudar a sostener la historia. También es mejor parecer abatido y no intimidatorio. Hablarle educadamente y no decir palabrotas también ayudará a que le caiga bien y sienta pena por usted. La llave USB debe contener un documento que se llame `miCV.doc` o `miCV.pdf` que sea imprimible. El formato PDF es el más utilizado, ya que la mayoría de empresas utiliza una versión antigua de Adobe Reader que es vulnerable a muchos tipos de explotación. Asegúrese de que el currículum está en un formato que pueda abrirse, no en un formato extraño.

Casi siempre, la gente quiere ayudar. Quieren ser capaces de asistir a una persona en apuros si la historia es creíble y conmovedora. Si lo desea, puede darle un giro a la historia: "Venía hacia aquí y era mi turno de dejar a mi hija en el colegio. Cuando se subió al asiento para darme un beso de despedida derramó el café en mi cartera. Ya llegaba tarde y estaba más cerca de aquí que de casa; ¿podría, por favor, imprimirme una copia nueva?".

De cualquier forma, esta historia suele funcionar y la llave USB acabará insertada en el ordenador comprometiendo el ordenador de la recepcionista, lo que podrá llevar a poner en peligro a toda la empresa.

El poder de los modelos de comunicación

El desarrollo de modelos de comunicación es una herramienta poderosa y una habilidad obligatoria de todo ingeniero social. La parte más difícil de la creación de un modelo es asegurarse de que sus sesiones de recopilación de información están bien hechas. En los dos escenarios explicados, no tener un plan y un modelo lo suficientemente buenos llevarán al fracaso. Una buena manera de practicar la creación de un modelo de comunicación es redactar un modelo de manipulación de una persona que conozca bien (la pareja, un hijo, el jefe, un amigo) para que lleve a cabo una acción concreta.

Establezca una meta que no sea malintencionada, por ejemplo conseguir que alguien esté de acuerdo en cambiar el lugar al que van a ir de vacaciones o en ir a un restaurante que le gusta pero que su pareja odia o que le permita gastar dinero en algo en lo que normalmente no lo haría. Sea lo que sea lo que decida, escriba los cinco componentes de la comunicación y compruebe después cómo evoluciona cuando tiene un plan escrito. Descubrirá que, con sus metas bien definidas, podrá probar mejor sus métodos de comunicación y ser capaz de lograr sus metas más fácilmente. Haga una lista con los siguientes cinco puntos y después vaya completándolos uno a uno, conectando los puntos mientras avanza.

- Fuente.
- Mensaje.
- Canal.
- Receptores.
- Retroalimentación.

Los modelos proporcionan información muy valiosa y sin ellos la comunicación no será efectiva. Como expliqué anteriormente, la recopilación de datos es el quid de toda acción de ingeniería social, pero si domina la recopilación de información y es capaz de reunir increíbles cantidades de datos pero no sabe cómo utilizarlos, habrá sido una pérdida de tiempo.

Aprenda a ser un maestro en la recopilación de información y después practique poniéndola en acción con modelos de comunicación. Esto es sólo el comienzo, pero puede cambiar literalmente el modo en que trata con la gente, tanto como ingeniero social como en el día a día. Aun así, se necesita mucho más para desarrollar un mensaje sólido en un modelo de comunicación.

Un aspecto clave para aprender a comunicar, manipular y a ser un ingeniero social es aprender a utilizar las preguntas, como se explica en el siguiente capítulo.

3. Las maniobras de obtención de información

El supremo arte de la guerra consiste en someter al enemigo sin luchar.
Sun Tzu

Conseguir sonsacar a la gente de manera efectiva es una habilidad clave para un ingeniero social. Cuando la gente esté hablando con usted debe sentirse cómoda y con ganas de abrirse.

¿Alguna vez ha conocido a alguien y ha pensado enseguida: "Vaya, me gusta esta persona"? ¿Por qué? ¿Qué tenía esa persona para hacerle sentir de esa manera? ¿Era su sonrisa? ¿Su aspecto? ¿El modo en que le trataba? ¿Su lenguaje corporal?

Quizá tenía incluso la sensación de que "sintonizaba" con sus pensamientos y deseos. Esa persona le trató sin hacer juicios de valor y enseguida se sintió cómodo con ella.

Ahora imagine que puede aprender a dominar esa habilidad. No menosprecie este capítulo pensando que es una simple lección sobre "cómo generar compenetración". Este capítulo es sobre las maniobras de obtención de información, una poderosa técnica utilizada por espías, estafadores e ingenieros sociales, así como por médicos, terapeutas y agentes de las fuerzas del orden y si lo que quiere es estar protegido o llegar a ser un gran auditor debe dominar esta técnica. Utilizadas de forma efectiva, estas maniobras pueden producir resultados increíbles.

¿Qué son las maniobras de obtención de información? Muy pocos aspectos de la ingeniería social son tan poderosos. Ésa es una de las razones por la que están en lo más alto del ámbito conceptual. Esta técnica por sí sola puede cambiar el modo en que la gente le ve. Desde el punto de vista de la ingeniería social, puede cambiar la forma en la que enfoca la seguridad.

Este capítulo analiza ejemplos de maniobras y explica cómo utilizar esta poderosa habilidad.

Antes de profundizar demasiado, hay que empezar por lo básico.

¿Qué son las maniobras de obtención de información?

Las maniobras de obtención de información consisten en provocar o sonsacar o llevar a una conclusión (a la verdad, por ejemplo) a alguien a través de la lógica. También pueden entenderse como una estimulación que expone (o saca a la luz) una clase de conducta particular.

Lea esa definición otra vez y, si no le pone la carne de gallina, puede que tenga un problema. Piense en lo que significa. Ser capaz de utilizar de forma efectiva estas maniobras significa que podrá formular preguntas que pueden sonsacar a la gente y empujarlas a adoptar el comportamiento que usted quiera. Como ingeniero social, ¿esto qué quiere decir? Ser eficaz sonsacando información significa que puede escoger sus palabras y plantear sus preguntas de tal manera que llevará sus capacidades a nuevos niveles.En términos de recopilación de información, las maniobras pueden traducirse en que su objetivo estará "deseando" contestar todas sus preguntas.

Quiero llevar la explicación un poco más allá porque muchos gobiernos forman a sus empleados advirtiéndoles en contra de estas maniobras porque son utilizadas por los espías en todo el mundo.

En sus materiales formativos, la Nacional Security Agency (Agencia de seguridad nacional) del gobierno de Estados Unidos define las maniobras de obtención de información como "la extracción sutil de información durante una conversación aparentemente normal e inocente".

Estas conversaciones pueden ocurrir en cualquier lugar en el que se encuentre el objetivo: un restaurante, un gimnasio, una guardería. Cualquier sitio. Las maniobras funcionan muy bien porque son poco arriesgadas y difíciles de detectar. La mayor parte del tiempo, las víctimas no saben dónde se está produciendo la fuga de información. Incluso si se levanta la sospecha de perseguir algún propósito dudoso, ésta se puede esquivar interpretando el papel de un extraño que

se enfada por ser acusado de tener malas intenciones simplemente por hacer una pregunta. Las maniobras de obtención de información funcionan bien por varias razones:

- La mayoría de la gente tiene el deseo de ser cordial, especialmente con extraños.
- Los profesionales quieren parecer inteligentes y bien informados.
- Si le dedica elogios a la gente, seguramente hablará más y divulgará más cosas.
- La mayoría de la gente no miente por mentir.
- La mayoría de las personas responde amablemente ante quienes parecen preocupados por ellas.

Estos hechos clave sobre la mayoría de seres humanos son la razón por la que las maniobras funcionen tan bien. Es muy fácil conseguir que la gente hable de sus logros. En una situación en la que me encargaron reunir información sobre una empresa, me encontré con mi objetivo en una reunión de la cámara de comercio. Era una fiesta con baile, así que me mantuve rezagado hasta que vi al objetivo acercarse a la barra. Llegamos al mismo tiempo y, como el propósito de estas reuniones es conocer y saludar a la gente e intercambiar tarjetas de visita, mi primer movimiento no fue complicado.

Dije: "Qué, ¿huyendo de los buitres?".

Respondió, con una risita entre dientes: "Sí, esto es lo único que merece la pena, la barra libre".

Esperé a que pidiera su bebida y pedí una parecida. Me acerqué con la mano extendida y dije: "Paul Williams".

"Larry Smith".

Saqué una tarjeta de visita que había encargado por Internet. "Trabajo en una pequeña empresa de importaciones como jefe de compras".

Mientras me daba su tarjeta, dijo: "Yo soy director de finanzas de XYZ".

Con una sonrisa, contesté: "¡Ah! Tú eres el que maneja la pasta, por eso todos te persiguen. ¿Qué es lo que hacéis exactamente?".

Empezó a explicarme algunos detalles sobre los productos de su empresa y cuando mencionó uno que es muy conocido, dije: "Ah, sí, vosotros hacéis ese 'chisme'; me encanta. Leí en la revista *XYZ* que erais récord de ventas gracias a él". A raíz de mi recopilación de información previa, sabía que él tenía un interés personal en ese producto, por lo que mi elogio fue bien recibido.

Empezó a hinchar el pecho un poco. "¿Sabías que ese aparato vendió más en el primer mes que nuestros cinco productos anteriores y posteriores juntos?"

"¡Vaya! Bueno, no me extraña. Yo mismo me he comprado cinco". Sonreí para acompañar el suave elogio.

Después de otra copa y un poco más de tiempo, descubrí: que habían comprado un software de contabilidad recientemente, el nombre del jefe de ventas (y el hecho de que estaba de vacaciones) y que mi nuevo amigo también se iba pronto de vacaciones a las Bahamas con su mujer.

Esta información aparentemente inútil no lo es en absoluto. Tenía una lista de detalles sobre software, personas y vacaciones que podía ayudarme a planear mi ataque. Pero no quería detenerme aquí; fui a por todas con esta pregunta:

"Sé que esta pregunta te parecerá extraña, pero somos una empresa pequeña y mi jefe me ha pedido que investigue y que compre un sistema de seguridad para las puertas. Por ahora sólo utilizamos llaves pero está pensando en instalar un sistema de RFID o algo por el estilo. ¿Tú sabes qué sistema utilizáis vosotros?"

Pensé que esta pregunta haría saltar las luces de emergencia. Sin embargo, dijo: "No tengo ni idea. Yo sólo firmo los cheques que lo pagan. Lo único que sé es que tengo esta curiosa tarjeta..." y sacó su cartera para enseñarme la tarjeta. "Creo que es de RFID, pero todo lo que sé es que paso mi cartera por delante de un pequeño dispositivo y la puerta se abre".

Intercambiamos unas risas y me fui con una información que me proporcionaba unos vectores de ataque que suelen ser muy exitosos. Como habrá observado, las maniobras de obtención son muy parecidas y están conectadas con la recopilación de información. Esta sesión de recopilación fue mucho más sencilla gracias a un pretexto sólido (explicado en el capítulo 4) y a unas buenas habilidades para sonsacar información. Estas habilidades son las que lograron que las preguntas fluyeran suavemente y que el objetivo se sintiera cómodo contestándolas.

Sabiendo que estaba de vacaciones y los tipos de software de contabilidad y de sistemas de seguridad que usaban en las puertas, pude planificar una visita in situ para reparar un dispositivo de control de RFID "defectuoso". Sencillamente me acerqué a la recepcionista y dije: "Larry me llamó antes de irse a las Bahamas y me comentó que había un dispositivo de control en el departamento de fabricación que no está funcionando correctamente. Sólo me llevará unos minutos comprobarlo y analizarlo". Me dieron acceso en cuestión de segundos sin hacerme preguntas.

Las maniobras de obtención de información me llevaron a este éxito porque con todos los datos que había obtenido la recepcionista no tenía motivo para dudar de mi pretexto. Una conversación sencilla, ligera y despreocupada es todo lo que se necesita para sonsacar a la gente una información valiosa. Como ya hemos explicado, definir sus metas es fundamental para lograr los mejores resultados. Las maniobras no se utilizan solamente para la recopilación de información, también pueden utilizarse para consolidar su pretexto y conseguir acceso a los datos. Todo dependerá de un modelo de maniobras bien pensado y claramente definido.

Las metas de las maniobras de obtención de información

Revisar la definición de las maniobras puede aclararle cuáles son sus metas. Sin embargo, todo se puede reducir a una cosa. Un ingeniero social quiere que el objetivo realice una acción, ya sea una acción tan simple como contestar a una pregunta o tan compleja como permitir el acceso a una zona restringida. Para conseguir que el objetivo acceda, se formularán una serie de preguntas o se mantendrá una conversación que llevará al objetivo por ese camino.

La información es la clave. Cuanta más reúna, más exitoso será el ataque. Las maniobras funcionan bien porque no son amenazantes. Haga la cuenta de las veces a la semana que mantiene pequeñas conversaciones insignificantes con alguien en una tienda, cafetería o cualquier otro sitio. Las maniobras se basan en la metodología de esas conversaciones y se utilizan de un modo inofensivo a diario. Por eso son tan efectivas.

En la popular serie de la televisión británica *The Real Hustle*, los presentadores demuestran la sencillez de muchos ataques de ingeniería social. En un episodio, la meta era involucrar a la víctima en un juego de azar amañado. Para lograrlo, un cómplice actuaba como un completo extraño que mostraba interés y mantenía una conversación con el atacante. Esta conversación atraía a la gente de alrededor, con lo que se conseguía sonsacar las respuestas adecuadas a la víctima muy fácilmente. Éste es un método muy efectivo.

Cualquiera que sea el método que utilice, la meta es obtener información y después utilizarla para conducir al objetivo por el camino que el ingeniero social quiere que siga. Comprender esto es importante. En capítulos posteriores, explicamos el pretexto y otras tácticas de manipulación, pero no debe confundir las maniobras de obtención de información con esas tácticas. Es importante comprender que las maniobras son conversación. Por supuesto están muy relacionadas con el pretexto, el lenguaje corporal y los movimientos oculares, pero todo esto pierde importancia en comparación a su habilidad para captar a alguien en una conversación.

Algunos expertos están de acuerdo en que existen tres pasos para dominar el arte e la conversación:

1. **Sea natural:** Nada puede arruinar una conversación más rápidamente que parecer incómodo o artificial durante la misma. Para comprobar esto por sí mismo, pruebe este ejercicio. Mantenga una conversación con alguien sobre algún tema del que usted sepa mucho. Si puede, grábelo de alguna forma o consiga que alguien tome notas de sus reacciones y después analice cómo se mueve, su postura, cómo afirma su conocimiento. Todos estos detalles dan

muestra de confianza y naturalidad. Después participe en una conversación sobre un tema del que no sabe nada y vuelva a grabarlo o vuelva a hacer que alguien le observe y tome nota. Compruebe cómo todos esos aspectos no verbales cambian en usted cuando intenta aportar un comentario inteligente a una conversación de la que no sabe nada.

Este ejercicio le muestra la diferencia entre ser natural y no serlo. Las personas con las que converse serán capaces de verlo muy fácilmente, lo que arruinará todas sus opciones de tener éxito. ¿Cómo conseguir ser natural en una conversación? Así llegamos al segundo paso.

2. **Fórmese:** Debe conocer aquello de lo que va a hablar con sus objetivos. Esta sección debería venir marcada con una enorme señal luminosa de advertencia, pero como no todos los libros pueden tener una, permítame enfatizar esta parte.

   Es "imprescindible" que no pretenda ser más de lo que razonablemente la gente puede creer que es.

   ¿Confundido? Aquí tiene un ejemplo para aclararlo. Si quisiera conseguir la composición química de un producto de alto secreto y su objetivo es uno de los químicos implicados en su elaboración y decide empezar a hablar de química, no interprete el papel de un químico experimentado (a no ser que lo sea). Puede que el objetivo le haga alguna pregunta que ponga de manifiesto que no sabe nada, derribando su cobertura y su plan.

   Un método más realista podría ser que usted es un investigador en prácticas estudiando cierto asunto y le han comentado que el objetivo sabe mucho sobre ese tema. Debido a su experiencia, quería preguntarle unas dudas sobre una fórmula química en la que está trabajando y pedirle ayuda para saber por qué no consigue que funcione.

   La cuestión es que, sea cual sea el tema y la persona con la que elija conversar, investigue, practique y esté preparado. Tenga el conocimiento suficiente para hablar con coherencia sobre un tema que interese a su objetivo.

3. **No sea avaricioso:** Por supuesto, la meta es "conseguir" información, "conseguir" respuestas y "conseguir" las "llaves del cielo". Aun así, no deje que toda la conversación vaya en esa dirección. Enseguida se hará evidente que sólo está ahí por intereses personales y el objetivo perderá interés. A menudo, dar algo a alguien suscita el sentimiento de reciprocidad (explicado en el capítulo 6), por el que él o ella siente ahora la obligación de darle algo a cambio. Es importante actuar de esta forma. Haga que la conversación sea

un dar y tomar, a no ser que a la persona con la que conversa le guste dominar la conversación. Si le gusta dominar, déjela. Pero si obtiene algunas respuestas vaya regulando la presión que ejerce, no se vuelva avaricioso intentando profundizar más y más, puede hacer saltar las alarmas.

Muchas veces las personas que son etiquetadas como "buenas conversadoras" son aquéllas que se dedican más a escuchar que a hablar.

Estos tres pasos para sonsacar información con éxito pueden cambiar literalmente la forma en que conversa con la gente a diario y no sólo como auditor de seguridad, sino como una persona cualquiera. Personalmente, me gusta añadir uno o dos más a estos pasos.

Por ejemplo, un aspecto importante de las maniobras de obtención de información durante una conversación son las expresiones faciales. Si su mirada es demasiado intensa o demasiado relajada puede afectar al modo en que la gente reacciona a sus preguntas. Si habla con tranquilidad y ha conseguido atraer a su objetivo a una conversación pero su lenguaje corporal o sus expresiones faciales muestran desinterés, esto puede afectar al ánimo de la persona con la que conversa, aunque sea de forma inconsciente.

Aunque esta afirmación parezca un poco rara en este momento, soy un gran admirador de César Millán, alias *The Dog Whisperer* (el encantador de perros). Creo que ese hombre es un genio. Coge a un perro que parece incontrolable y en cuestión de minutos consigue que afloren en el perro y en su dueño rasgos de su personalidad gracias a los cuales su relación mejorará sensiblemente. Básicamente, enseña a la gente a comunicarse con los perros (cómo pedirles que hagan cosas en un lenguaje que entienden). Una de las cosas que afirma, con la que estoy totalmente de acuerdo, es que el "espíritu" o energía de la persona afecta al "espíritu" o energía del perro. En otras palabras, si la persona se acerca al perro tenso y ansioso, aunque le hable con tranquilidad el perro también se mostrará tenso y nervioso y ladrará más.

Evidentemente, las personas no son iguales que los perros pero creo firmemente que se puede aplicar esta misma filosofía. Cuando un ingeniero social se acerca a su objetivo, su "espíritu" o energía afecta la percepción de esa persona. La energía se manifiesta a través del lenguaje corporal, la expresión facial, la vestimenta y las palabras que respaldan todo lo demás. La gente percibe todas estas cosas incluso sin darse cuenta. ¿Alguna vez ha pensado o ha oído a alguien decir: "Ese hombre me da escalofríos" o "Parece una buena chica"?

¿Cómo funciona este concepto? El espíritu o energía de una persona se transmite a los "sensores" de la otra, que relaciona esa información con sus experiencias pasadas y entonces forma una opinión. La gente realiza este proceso de manera instantánea, casi siempre sin darse cuenta. Por lo tanto, cuando inicie una maniobra

para obtener información de alguien, su energía debe corresponderse con el papel que vaya a representar. Si su personalidad o su estructura mental no le permiten representar el papel de un gerente con facilidad, entonces no lo intente. Trabaje con lo que tiene. Yo siempre he sido una persona sociable y mis puntos fuertes no son temas como la química o las matemáticas avanzadas. Si yo estuviera en la situación mencionada previamente no intentaría interpretar el papel de una persona que sabe de esas cosas. Mi maniobra sería tan sencilla como representar a un desconocido interesado en iniciar una conversación sobre el tiempo.

Independientemente de los métodos que prefiera utilizar, hay ciertos pasos que puede dar para tomar ventaja. Uno de esos pasos es la "carga previa".

La carga previa

Hace cola en el cine para comprar su billete de 10 euros y recibe una sobrecarga sensorial de carteles de próximos estrenos de películas. Hace cola para gastarse 40 euros en palomitas y refrescos y ve más carteles. Finalmente, se abre paso a empujones para conseguir un asiento. Antes de que empiece la película proyectan unos tráiler de futuros estrenos. Algunas de esas películas ni siquiera están en producción todavía, pero el locutor anuncia: "La película más divertida desde..." o empieza una música siniestra, una densa niebla cubre la pantalla y una voz en *off* dice: "Pensaste que todo había terminado en *El asesino del parque 45*...".

. Sea la película que sea, los publicistas le están diciendo lo que debe sentir. En otras palabras, están realizando sobre usted una carga de lo que debe pensar sobre esta película antes de que empiece el tráiler. Después, utilizan los siguientes dos o tres minutos para mostrarle secuencias que despierten su deseo de ver la película y que atraigan a la audiencia que le gusta la historia de terror, el romance o la comedia.

No se ha escrito mucho sobre la carga previa, pero es un tema muy serio. Significa que puede hacer precisamente eso: cargar por anticipado a sus objetivos con información o ideas sobre cómo quiere que reaccionen ante cierta información. Se utiliza a menudo en los mensajes publicitarios; por ejemplo, en los anuncios de cadenas de restaurantes que muestran a gente guapa riendo y disfrutando de esa comida que tiene tan buena pinta. Cuando exclaman: "¡Hummm...!" y "¡Ooo...!" casi puede saborear la comida.

Por supuesto, como ingeniero social no puede realizar un anuncio para sus objetivos, así que, ¿cómo puede utilizar la carga previa?

Como en muchos aspectos de la ingeniería social, debe empezar por el resultado final y trabajar hacia atrás. ¿Cuál es su meta? Puede tener una meta clásica de las maniobras de obtención de información como es sonsacarle información al

objetivo sobre un proyecto en el que está trabajando o las fechas en las que estará en la oficina o de vacaciones. Sea lo que sea, lo primero que debe hacer es concretar la meta que persigue. Después, debe decidir el tipo de preguntas que quiere realizar y también qué tipo de información se puede cargar a una persona para que después quiera contestar a esas preguntas.

Por ejemplo, si le apetece ir a cenar un entrecot a un asador que a su mujer no le gusta mucho, puede llevar a cabo una carga previa sobre ella para conseguir lo que quiere. Durante el día puede decir, por ejemplo: "Cariño, ¿sabes lo que me apetece? Un buen filete a la brasa bien grande y jugoso.

El otro día conducía hacia la oficina de correos y pasé por delante del jardín de Fred. Había sacado la parrilla y justo en ese momento acababa de empezar a hacer los filetes a la brasa y me llegó ese olor que me está persiguiendo desde entonces". No importa si no obtiene una respuesta en ese preciso instante; ha conseguido plantar una semilla que ha estimulado todos los sentidos de su mujer. Ha hecho que se imagine la carne crepitando en la parrilla, le ha descrito el proceso, le ha hablado del olor del humo y de lo mucho que le apetece un filete como ésos.

Imagine que más tarde trae a casa el periódico y en su interior encuentra un anuncio del restaurante al que quiere ir con un cupón de descuento. Simplemente deja la página abierta sobre la mesa. Puede que su mujer lo vea o puede que no, pero hay muchas opciones de que lo haga porque ha dejado el periódico junto al correo, porque ha mencionado el entrecot y porque sabe que a su mujer le gustan los cupones de descuento.

Más tarde, ella le pregunta:" ¿Qué quieres cenar esta noche?". Aquí es donde la carga previa entra en juego; ha mencionado el olor, la imagen de la parrilla y su deseo por un entrecot. Ha dejado un cupón del restaurante a la vista sobre la mesa y ahora es el momento de hablar de la cena. Le contesta: "En vez de cocinar y tener que recoger y limpiar la cocina después, hace mucho que no vamos al restaurante XYZ. ¿Por qué no vamos esta noche?".

Como sabe que a ella no le gusta ese restaurante, lo único que puede hacer es esperar que la carga previa haya hecho efecto. Ella contesta: "He visto un cupón en el periódico. Con una cena te regalan la mitad de otra. Pero ya sabes que no me gusta...".

Puede interrumpirla mientras habla con un elogio: "¡Ja! La reina de los cupones ataca de nuevo. Vaya, sé que no te gusta mucho la carne pero Sally me dijo que también tienen un pollo buenísimo".

Unos minutos más tarde, está de camino al paraíso de la carne. Mientras que un ataque frontal expresando su deseo de ir a XYZ seguramente hubiera recibido como respuesta un rotundo "¡no!", la carga previa ha preparado la mente de su mujer para aceptar su propuesta y ha funcionado.

Pongamos otro ejemplo muy simple antes de continuar avanzando: Un amigo le dice: "Tengo que contarte una historia divertidísima". ¿Cómo reacciona? Puede que incluso empiece a sonreír antes de que empiece a contar la historia. Su previsión es escuchar algo muy divertido por lo que está pendiente, esperando la oportunidad para empezar a reírse. Su amigo le ha hecho una carga previa y usted se ha adelantado a la historia divertida.

¿Cómo funcionan estos principios en el ámbito de la ingeniería social?

La carga previa es una habilidad en sí misma. Ser capaz de implantar ideas o pensamientos sin que resulte obvio o avasallador a veces requiere más habilidad que las propias maniobras de obtención de información. Otras veces, dependiendo de la meta, la carga previa puede ser un proceso bastante complejo. La situación del entrecot que hemos visto previamente, es un problema complicado. La carga requiere tiempo y energía. Una situación mucho más sencilla sería, por ejemplo, averiguar qué marca de coche conduce alguien o algún dato igual de inofensivo. En una conversación muy informal, en la que "por casualidad" está en la misma tienda que su objetivo, inicia una conversación desenfadada con algo así: "La verdad es que me encanta mi Toyota. Un tipo en un Chevrolet me acaba de dar un golpe en el aparcamiento y mi coche no tiene ni un arañazo". Con un poco de suerte, si atrae a su objetivo a una conversación, su afirmación sobre su coche puede prepararle para las preguntas que le quiere hacer sobre marcas de coches o cualquier otro tema del que quiera reunir información.

El tema de la carga previa tiene más sentido cuando analiza cómo puede utilizar las maniobras de obtención de información. Todo ingeniero social domina esta habilidad. En muchas ocasiones, se da cuenta de que tiene este talento mucho antes de dedicar su vida al oficio. Siendo joven le resulta fácil interactuar con la gente y más tarde se da cuenta de que tiende a verse atraído por trabajos que requieren esa habilidad. Puede que sea la pieza central de su grupo de amigos y a la gente le resulte sencillo contarle todos sus problemas. Después, se da cuenta de que gracias a esta habilidad consigue cosas que de otra forma no podría conseguir.

De pequeño siempre tuve este talento. Mis padres me contaban cómo entablaba conversaciones con desconocidos cuando sólo tenía cinco o seis años, a veces incluso entrando en la cocina de restaurantes repletos para preguntar sobre la comida que habíamos pedido o sobre cómo preparaban los platos. De alguna forma siempre conseguía lo que quería. ¿Por qué? Posiblemente porque no sabía que esta conducta era inadecuada y porque lo hacía con confianza. Al hacerme mayor esta habilidad (o falta de miedo) entró plenamente en juego. También daba la sensación de que a la gente, a veces auténticos desconocidos, le gustaba contarme sus problemas y hablarme de sus asuntos. Me ocurrió una historia cuando tenía unos 17 años que puede ayudar a mostrar mi habilidad para utilizar no sólo la carga previa, sino también unas buenas maniobras de obtención de información.

Era un surfista empedernido y hacía todo tipo de trabajos extraños para costear mi afición (cualquier cosa desde repartidor de pizzas a cortador de fibra de vidrio o socorrista). Durante un tiempo me dediqué a hacer recados para mi padre que tenía una empresa de consultoría financiera. Entregaba documentos a sus clientes, recogía firmas y los traía de vuelta. Muchas veces algunos de los clientes se abrían conmigo y me contaban sus vidas, sus divorcios y sus éxitos y fracasos con los negocios. Normalmente, siempre empezaba con una pequeña charla en la que contaban lo mucho que les gustaba mi padre. En aquel momento nunca llegué a comprender por qué la gente, especialmente adultos, decidían contarle a un chico de 17 años los motivos por los que su mundo se derrumbaba. Un cliente al que visitaba a menudo era dueño de una urbanización. No era una urbanización grande y lujosa; pero tenía unas cuantas propiedades y se encargaba de administrarlas. El pobre hombre tenía problemas serios: problemas familiares, de salud y personales, de los que me hablaba por costumbre tanto tiempo como yo estuviera dispuesto a quedarme escuchándole. Entonces fue cuando me di cuenta de que podía decir y hacer cosas increíbles simplemente por haber dedicado algún tiempo a escuchar a la gente. Les hacía sentir importantes y que yo era una buena persona. No importaba si yo estaba ahí sentado pensando en mi próxima ola; lo importante era que estaba escuchándoles.

Normalmente, escuchaba a este hombre hasta que ya no podía soportar más el humo del tabaco (fumaba más que cualquier persona que haya visto en toda mi vida). Pero siempre me sentaba y escuchaba y, como era joven y no tenía ninguna experiencia en la vida, no daba consejos ni proponía soluciones, sólo escuchaba. El caso es que los problemas de este hombre me preocupaban de verdad; no fingía. Deseaba poder ayudarle. Un día me dijo que lo más le gustaría era mudarse de vuelta al oeste, donde estaba su hija, para estar más cerca de su familia.

Yo quería progresar en la vida y conseguir un trabajo que me gustara, fuera divertido y me aportara el dinero que necesitaba para el surf y otras cosas que "necesitaba". Un día que estaba escuchando, se me ocurrió una idea descabellada que hizo que él me viera como un chico responsable y compasivo con la cabeza "bien amueblada". La carga había tenido lugar durante los meses previos que había pasado sentado escuchando. Ahora era el momento de sacar provecho de aquello. Dije: "¿Qué te parece si te mudas al oeste y yo me encargo de gestionar tu urbanización?". La idea era tan absurda, tan ridícula, que recordándola ahora estoy seguro de que yo me hubiera reído en mi cara. Pero había pasado semanas, incluso meses, escuchando sus problemas. Conocía bien a este hombre y conocía sus inquietudes. Además, nunca me había reído de él ni le había rechazado. Ahora me había contado un problema y yo había propuesto la solución perfecta, con la que se solucionaban todos sus problemas y los míos también. Mis necesidades económicas eran moderadas y él quería estar cerca de su familia. Habíamos construido una relación a lo largo de los últimos meses y gracias a eso él me "conocía" y confiaba en mí.

Discutimos el tema y llegamos a un acuerdo; él volvió al oeste y yo me convertí en un chico de 17 años que gestionaba una urbanización de 30 apartamentos como "ayudante del propietario". Podría continuar relatando muchos más detalles de esta historia, pero creo que ya he dejado clara la idea. (En resumen, el trabajo fue bien. Finalmente, me pidió que intentara vender la urbanización en su nombre. Conseguí venderla en tiempo récord, perdiendo mi trabajo al hacerlo).

El punto importante es que conseguí desarrollar compenetración y confianza con alguien y, sin proponérmelo ni esconder malas intenciones, durante meses realicé una carga sobre él con la idea de que yo era amable, compasivo e inteligente. Después, cuando se presentó la ocasión, propuse una idea absurda y, gracias a los meses de carga previa, fue aceptada.

Años más tarde comprendí lo que había sucedido. Había tantos factores en juego que en aquel momento no fui consciente de lo que pasaba. Desde el punto de vista de la ingeniería social, llevar a cabo una carga previa implica tener una meta antes de empezar. En este caso, yo no sabía que iba a acabar realizando este curioso trabajo para aquel hombre. Pero, aun así, la carga funcionó.

En la mayoría de situaciones, los resultados se obtienen con mucha más rapidez pero los principios que entran en juego son los mismos. Es fundamental ser lo más sincero posible. Teniendo en cuenta que entran en juego los sentimientos y los sentidos de la gente, no puede dejarse lugar a dudas. La pregunta que plantee tiene que tener relación con su pretexto. Para que la carga previa funcione, debe preguntar algo que tenga relación con la confianza que se ha generado. Por ejemplo, si yo le hubiera propuesto a este cliente ir a ver a su familia para hacerles unas fotos en vez de administrar su urbanización, esa oferta no hubiera tenido ninguna relación con la imagen que se había formado sobre mí: que era un chico listo y bondadoso, con dotes para los negocios. Por último, la oferta siempre debe consistir en algo que beneficie al objetivo o al menos que dé la impresión de que le beneficia. En mi caso, mi cliente se beneficiaba claramente del trato. Pero en ingeniería social el beneficio que obtiene puede ser tan limitado como, por ejemplo, darle al objetivo la oportunidad de que "presuma" un poco. O puede ser un beneficio mucho mayor de tipo físico, económico o psicológico. Practicar y dominar las maniobras de obtención de información le convertirán en un maestro de la ingeniería social. Por lo tanto, la siguiente sección explica cómo dominar estas maniobras.

Dominar las maniobras de obtención de información

Simplemente analizando mis propias experiencias puedo identificar los elementos fundamentales que me han conducido al éxito desde que tengo cinco años hasta ahora:

- Nunca he tenido miedo a hablar con la gente y a encontrarme en situaciones que no se consideran "normales".
- Verdaderamente me preocupo por las personas incluso cuando no las conozco. Me gusta y disfruto escuchando a la gente.
- Sólo doy consejos u ofrezco ayuda cuando tengo una solución real.
- Escucho los problemas de la gente sin hacer juicios de valor.

Éstos son elementos clave para tener éxito con las maniobras de obtención de información. El *United States Department of Homeland Security* (Departamento de seguridad nacional de Estado Unidos) redactó un folleto interno que distribuye entre todos sus agentes y que he archivado en `www.social-engineer.org/wiki/archives/BlogPosts/ocso-elicitation-brochure.pdf`.

Este documento contiene algunas sugerencias muy buenas. Básicamente, establece, al igual que este capítulo, que las maniobras de obtención de información son utilizadas porque funcionan, son muy difíciles de detectar y no son amenazantes. El folleto del Departamento de seguridad nacional aborda estas maniobras desde la perspectiva de "cómo evitarlas", pero la siguiente sección explica algunas de las situaciones posibles y le muestra lo que se puede aprender de ellas.

Apelar al ego de una persona

El escenario descrito en el folleto gubernamental dice así:

Atacante: "Debe usted tener un trabajo importante; el señor X parece tenerle en alta estima".

Objetivo: "Gracias, es usted muy amable, pero mi trabajo no es tan importante. Lo único que hago es...".

El método de apelar al ego de alguien es simplista pero efectivo. Aunque se requiere precaución: incidir sobre el ego de alguien es una herramienta poderosa pero, si abusa de ella o si la emplea sin sinceridad, la gente lo percibirá y no reaccionará. No debe parecer un acosador disparatado: "Oh, eres la persona más importante del universo y además eres tan guapa...". Diciendo cosas como ésta, lo único que conseguirá es que alguien llame al personal de seguridad.

Cuando apele al ego de alguien, debe hacerlo sutilmente y, si está hablando con una persona realmente narcisista, evite poner los ojos en blanco, suspirar o discutir cuando alardee sobre sus logros. Para apelar con sutileza al ego se pueden decir cosas como: "Aquella investigación que hiciste cambió realmente el punto de vista de mucha gente sobre..." o "He escuchado al señor Smith diciéndole a ese grupo de ahí que eres uno de los mejores analistas que tiene". Si hace una afirmación exagerada, resultará demasiado obvio.

Como indica el formulario, un halago sutil puede introducir a una persona en una conversación que de otra manera no hubiera tenido lugar y eso es justo lo que busca un ingeniero social.

Expresar interés mutuo

Imagine este escenario simulado:

Atacante: "Vaya, ¿tienes formación en bases de datos adecuadas a la norma ISO 9001? Deberías ver el modelo de motor de informes que hemos creado para ayudar con esa certificación. Si quieres puedo conseguirte una copia".

Objetivo: "Me encantaría echarle un vistazo. Llevamos un tiempo dándole vueltas a la idea de incluir un motor de informes en nuestro sistema".

Expresar interés mutuo es una maniobra de obtención de información importante. En este escenario concreto, es incluso más poderosa que apelar al ego de alguien porque amplía la relación más allá de la conversación inicial. El objetivo ha accedido a seguir en contacto, a aceptar software del atacante y ha expresado interés en discutir planes para el software de la empresa más adelante. Todo esto puede conducir a una gran brecha de seguridad. El peligro de esta situación es que ahora el atacante tiene el control absoluto. Controla el paso siguiente, qué información y cuánta va a enviar y cuándo lo hará. Una posición muy poderosa. Por supuesto, si se creara una relación a largo plazo, tener realmente el software que va a compartir sería todavía más ventajoso. Compartir software útil y no malicioso generará confianza, compenetración y hará que el objetivo se sienta obligado a corresponder.

Hacer una afirmación falsa intencionadamente

Puede pensarse que hacer una afirmación falsa es contraproducente, pero lo cierto es que puede ser un arma poderosa a tener en cuenta.

Atacante: "Todo el mundo sabe que la empresa XYZ lidera las ventas de software para este artilugio".

Objetivo: "Me temo que eso no es cierto. Nuestra empresa empezó a vender un producto similar en 1998 y nuestras ventas han superado a las suyas de manera constante en más de un 23 por 100".

Este tipo de afirmaciones, si se realizan de forma efectiva, pueden sonsacar una respuesta del objetivo con datos reales. La mayoría de la gente siente la necesidad de corregir una afirmación incorrecta. Es como si se sintieran retados a probar que tienen la razón. Parece que el deseo de informar a otros, mostrarse culto y entendido y no tolerar informaciones erróneas está en la naturaleza humana. Entender este rasgo de la conducta le proporciona una herramienta poderosa. Puede utilizar este método para sonsacarle información real y detallada a su objetivo o para averiguar en un grupo quién conoce más sobre un tema.

Ofrecer información voluntariamente

El folleto del Departamento de seguridad nacional hace un interesante apunte sobre un rasgo de la personalidad que muchos tenemos. Ya lo hemos mencionado alguna vez en el libro y más adelante lo explicamos con más detalle, se trata de la poderosa fuerza de la obligación, sentirse obligado a algo. Cuando en una conversación damos algún tipo de información, el objetivo se ve prácticamente obligado a responder con una información parecida.

¿Quiere comprobarlo? La próxima vez que esté con sus amigos pruebe a decir algo así: "¿Os habéis enterado de lo que le ha pasado a Ruth? Por lo visto, la han despedido y no consigue encontrar trabajo".

Seguramente alguien dirá algo como: "Vaya, no lo sabía. Qué mala noticia. Yo he oído que Joe se divorcia y además van a perder la casa".

Una triste faceta de la humanidad es que nos gusta confirmar el dicho de que "los males nunca vienen solos", como en este caso. La gente tiende a querer compartir noticias parecidas. Esta propensión puede utilizarse para establecer el tono de una conversación y crear un sentido de obligación.

El conocimiento asumido

Otra herramienta de manipulación poderosa es la del "conocimiento asumido". Es habitual asumir que, si una persona tiene conocimientos sobre un asunto concreto, se puede discutir ese asunto con ella. Un atacante puede sacar partido de esta característica presentando algún tipo de información como si él la conociera y llevando a cabo maniobras de obtención para construir una conversación a su alrededor. Después, puede repetir las ideas como si fueran suyas y continuar creando la ilusión de que conoce a fondo el tema. Ilustremos este concepto con un ejemplo.

En una ocasión tenía que viajar a China para negociar una serie de asuntos importantes. Necesitaba obtener información interna sobre la empresa objetivo involucrada en las negociaciones antes de reunirme con sus representantes. Nunca nos habíamos encontrado cara a cara pero fui a una conferencia en China antes de empezar las negociaciones. En la conferencia, escuché por casualidad una conversación en la que se hablaba sobre cómo tomar la delantera al negociar con los chinos.

Sabía que era mi oportunidad y, para poner las cosas todavía más interesantes, uno de los integrantes del grupo pertenecía a la empresa con la que tenía que reunirme. Rápidamente, me introduje en la conversación. Tenía que decir algo enseguida o quedaría en entredicho. Mi conocimiento sobre el tema era muy limitado, pero los demás no tenían porqué saberlo. En un momento de silencio empecé a hablar de la teoría Guanxi. Básicamente, esta teoría explica cómo dos personas,

no necesariamente del mismo estatus social, pueden entablar una relación en la que una de ellas se verá forzada a hacerle un favor a la otra. Expliqué cómo podía utilizarse esa relación y terminé enlazándolo con lo importante que era para mí no aceptar tarjetas de visita y simplemente guardarlas en el bolsillo, sino revisarlas, añadir comentarios y guardarlas en un lugar apropiado.

Esto bastó para hacerme parecer lo suficientemente entendido sobre el tema como para permanecer en el círculo de confianza que se había creado. Una vez que había establecido la base de mi conocimiento, me puse cómodo y me limité a escuchar cómo los demás explicaban su experiencia personal y su conocimiento sobre cómo negociar adecuadamente con las empresas chinas. Presté especial atención cuando habló el caballero que trabajaba para mi empresa objetivo. Me di cuenta de que los "consejos" que daba estaban íntimamente relacionados con la filosofía empresarial de su compañía. Esta información fue mucho más valiosa que cualquier otra que hubiera podido conseguir pagando y convirtió el viaje en todo un éxito.

Existe alguna situación más en la que se utilizan las maniobras de obtención de información.

Utilizar los efectos del alcohol

Nada suelta más la lengua que la bebida. Éste es un hecho desafortunado pero cierto. Si a cualquiera de las cinco situaciones precedentes les añade alcohol, sus efectos se multiplican por diez.

Seguramente la mejor manera de describir este concepto es como parte de una historia real.

En 1980 un científico del Laboratorio Nacional de Los Álamos viajó a un centro de investigación de China para hablar de su especialidad, la fusión nuclear. Tenía mucha información sobre las armas nucleares estadounidenses pero sabía que en ese viaje se estaba poniendo en una situación delicada y estaba determinado a ceñirse al asunto de su visita.

Sin embargo, era abordado con preguntas cada vez más concretas directamente relacionadas con las armas nucleares. La táctica de los atacantes cambió y comenzaron a hacerle muchas preguntas sobre fusión y astrofísica, sus especialidades.

Entonces, celebraron una fiesta en su honor. Le agasajaron y aplaudieron sus conocimientos y sus investigaciones, brindando en cada ocasión. Empezaron a preguntarle por asuntos secretos como las condiciones de ignición del deuterio y el tritio, los dos componentes de la entonces nueva bomba de neutrones. Se manejó bien esquivando las preguntas, pero después de varios brindis y una fiesta en su honor, decidió ofrecerles una analogía. Explicó al grupo que si se metían

esos dos componentes dentro de una bola que después se hacía rodar hasta que cayera de la mesa, probablemente prendieran fuego porque tenían un umbral de temperatura realmente bajo.

Esta información aparentemente insignificante seguramente provocó que los investigadores chinos encontraran un camino para la investigación en armas nucleares. Mostrarían esa información a otro científico y usarían el nuevo conocimiento para avanzar a la siguiente fase. Tras varios intentos, es muy probable que los científicos chinos tuvieran una idea clara del camino a seguir.

Éste es un ejemplo serio de cómo conseguir una imagen clara de la respuesta final utilizando las maniobras de obtención de información. Esto puede suceder en cualquier situación de ingeniería social. Puede que todas las respuestas no vengan de una misma fuente. Puede sonsacarle información a una persona sobre una fecha concreta, después utilizar ese dato para sonsacar otro en la fase siguiente y así en adelante. Conectar esos bloques de información suele ser la parte más complicada para perfeccionar estas habilidades. Éste es el tema que explicamos a continuación.

Hacer preguntas inteligentes

Ya se habrá dado cuenta de que su meta con las maniobras de obtención de información no consisten en acercarse a alguien y decir: "¿Cuál es la contraseña de vuestros servidores?".

La meta es conseguir pequeñas porciones de información aparentemente inútiles que le ayuden a hacerse una idea clara de las respuestas que busca o del camino para llegar a esas respuestas. En cualquier caso, este tipo de recopilación de información ayuda a encontrar un camino muy definido hacia la meta.

¿Cómo sabe qué tipo de preguntas formular?

La siguiente sección analiza los tipos de preguntas que existen y cómo pueden utilizarse.

Preguntas abiertas

Las preguntas abiertas no pueden responderse con un sí o un no. Preguntar: "¿Hace frío hoy, verdad?" dará como respuesta "sí", "ajá" o alguna afirmación parecida, mientras que preguntando:"¿Qué te parece el tiempo que hace hoy?" conseguirá una respuesta real: la persona tendrá que contestar con algo más que sí o no.

Una manera de aprender a utilizar las preguntas abiertas es estudiando y analizando a los buenos periodistas. Estos profesionales deben utilizarlas constantemente para obtener respuestas de sus entrevistados.

Imagine que tenía planes para quedar con un amigo pero éste los cancela y quiere saber por qué. Puede decir algo así: "Tengo curiosidad por saber qué pasó con nuestros planes del otro día".

"Me encontraba mal".

"Bueno, espero que estés mejor. ¿Qué te pasaba?".

Este tipo de preguntas normalmente dará mejores resultados que abalanzarse sobre la persona diciendo: "¿Qué pasa contigo, tío? ¡Me dejaste muy tirado el otro día!".

Otro aspecto efectivo de las preguntas abiertas es el uso de los términos "por qué" y "cómo". Ampliar una pregunta con "por qué" o "cómo" puede conducirle a una explicación más profunda de lo que preguntó inicialmente.

Estas preguntas tampoco se puede contestar con "sí" o "no" y el interlocutor puede revelar algunos detalles interesantes.

En ocasiones, las preguntas abiertas pueden encontrar cierta resistencia, por lo que puede ser bueno utilizar el "enfoque piramidal". Consiste en comenzar con preguntas concretas y continuar con preguntas más amplias cada vez. Para dominar esta técnica le sugiero que aprenda a utilizarla con adolescentes.

Por ejemplo, muchas veces una pregunta abierta como: "¿Qué tal hoy en el colegio?" obtendrá como respuesta un escueto "bien" y nada más. Hacer una pregunta concreta puede abrir mejor el flujo de información.

"¿Qué estáis haciendo en matemáticas este año?". Ésta es una pregunta muy concreta y sólo puede responderse de una forma muy precisa: "Álgebra 2".

"Ah, yo odiaba eso. ¿A ti te gusta?".

A partir de ahí puede ir ampliando sus preguntas y, una vez que consiga hacer hablar al objetivo, cada vez será más fácil ir obteniendo información.

Preguntas cerradas

Obviamente, las preguntas cerradas son lo contrario a las preguntas abiertas, pero son un modo muy efectivo de conducir a su objetivo donde desea. Normalmente, las preguntas cerradas no se pueden contestar con más de una o dos posibilidades.

Una pregunta abierta puede ser: "¿Qué relación tiene con su supervisor?", pero una pregunta cerrada se formularía así: "¿Tiene una buena relación con su supervisor?".

En las preguntas cerradas, la meta normalmente no es obtener información detallada; la meta es más bien dirigir al objetivo.

Las fuerzas de orden público y los abogados utilizan este tipo de razonamiento. Si quieren conducir a su objetivo por un camino concreto, formulan preguntas muy cerradas que no les otorgan libertad para contestar. Por ejemplo:

"¿Conoce al acusado, el señor Smith?".
"Sí, lo conozco".
"En la noche del 14 de julio, ¿vio al señor Smith en la taberna X?".
"Sí".
"¿A qué hora?".
"A las doce menos cuarto de la noche".

Todas éstas son preguntas muy cerradas que sólo permiten uno o dos tipos de respuesta.

Preguntas conductoras

Las preguntas conductoras son una combinación de las preguntas abiertas y las cerradas. Son preguntas abiertas pero con una insinuación que conduce hacia la respuesta. Por ejemplo: "Usted estaba a las doce menos cuarto de la tarde del 14 de julio con el señor Smith en la taberna X, ¿verdad?". Este tipo de pregunta conduce al objetivo donde se desea pero también le ofrece la oportunidad de expresar su punto de vista, aunque de forma muy limitada. También se carga al objetivo con la idea de que ya tiene conocimiento de los eventos por los que está preguntando.

Muchas veces las preguntas conductoras pueden contestarse con un sí o un no, pero son diferentes de las cerradas porque se incluye más información en la pregunta y, al contestarse, se obtienen más datos con los que trabajar. Estas preguntas afirman unos hechos y luego preguntan al objetivo si está o no de acuerdo con ellos.

En 1932, el psicólogo británico Frederic C. Bartlett realizó un estudio sobre la memoria reconstructiva. Le contaba una historia a los sujetos y después les pedía que dijeran lo que recordaban de ella inmediatamente después, otra vez al cabo de dos semanas y de nuevo al cabo de cuatro semanas. Bartlett descubrió que los sujetos modificaban la historia en base a su cultura, sus creencias y su personalidad. Ninguno fue capaz de recordar la historia con precisión ni completa. Concluyó que los recuerdos no son hechos precisos de nuestro pasado. Al parecer, los humanos intentamos que la memoria encaje en nuestra representación actual del mundo. Cuando se nos hacen preguntas muchas veces contestamos a partir de nuestros recuerdos basados en lo que es importante para nosotros.

Por este motivo, es posible formular preguntas mixtas a la gente y manipular sus recuerdos. Elizabeth Loftus, una investigadora líder en el campo de los testimonios de testigos visuales, ha demostrado a través del uso de las preguntas conductoras lo sencillo que resulta distorsionar el recuerdo que tiene una persona sobre un evento. Por ejemplo, si le muestra a una persona la foto del cuarto de un niño en la que no aparece ningún osito de peluche y luego le pregunta "¿has visto "un" osito de peluche?", no está insinuando que había uno en la habitación y la persona es libre de responder lo que le parezca. Sin embargo, si pregunta "¿has visto "el" osito de

peluche?" está insinuando que hay uno en la habitación y es más probable que la persona contesté "sí" porque la presencia de un osito es coherente con el esquema mental que una persona tiene del cuarto de un niño.

Gracias a estas investigaciones, la utilización de preguntas conductoras puede ser una herramienta muy poderosa. Aprender a dirigir al objetivo también puede mejorar la habilidad del ingeniero social para recopilar información.

Preguntas de conocimiento asumido

Las preguntas de conocimiento asumido son precisamente eso: preguntas en las que asume que el objetivo posee cierta información. La forma de determinar si el objetivo posee la información que se busca es haciendo una de estas preguntas.

Por ejemplo, una técnica empleada por las fuerzas de orden público es asumir que el objetivo ya sabe algo (de una persona, por ejemplo) y preguntar: "¿Dónde vive el señor Smith?". Dependiendo de la respuesta, el agente puede determinar hasta qué punto conoce a esa persona el objetivo. Un punto importante a tener en cuenta es que al utilizar las preguntas de conocimiento asumido nunca se le debe dar al objetivo una idea completa de lo que se busca o se pregunta. Hacer esto daría todo el poder al objetivo y privaría al ingeniero social de controlar el entorno. No deben utilizarse este tipo de preguntas para probar que el objetivo está equivocado. Hacerlo también le haría perder poder y alienaría al objetivo.

Las preguntas de conocimiento asumido deben utilizarse cuando se tenga una idea sobre los hechos reales que puede utilizar. Formular una pregunta con información falsa puede distanciar al objetivo y sólo confirmará que el objetivo no sabe nada sobre algo que nunca ocurrió. Volviendo a un ejemplo anterior, si quiero obtener información de un químico y he investigado y sé lo suficiente como para articular una frase inteligente podría formular una pregunta de conocimiento asumido pero esto podría arruinar el futuro del cuestionario si no puedo respaldarla cuando el objetivo asuma que tengo ciertos conocimientos.

Si pregunto, por ejemplo: "Ya que el deuterio y el tritio tienen esos umbrales de temperatura tan bajos, ¿cómo se manipulan esos materiales para no provocar su ignición?", la respuesta probablemente dará pie a una conversación difícil de seguir y no soy un físico nuclear. Esto sería contraproducente e inútil. Planee sus preguntas para que tengan el máximo efecto posible.

Un truco muy útil que les enseñan a los agentes de las fuerzas del orden es decir una frase como ésta: "Piense muy bien lo que va a decir antes de contestar la siguiente pregunta". Esta frase carga la mente del objetivo con la idea de que debe ser sincero con su siguiente contestación.

Puede llevar meses o incluso años dominar estas habilidades. No se desanime si los primeros intentos no dan frutos; siga intentándolo. Por suerte, existen algunos trucos para dominar esta habilidad. Los estudiaremos en profundidad.

Dominar las maniobras de obtención de información

Este capítulo contiene mucha información y si no es una persona especialmente sociable puede que utilizar las técnicas que se explican aquí le resulte una tarea complicada. Como la mayoría de aspectos de la ingeniería social, las maniobras de obtención de información tienen una serie de principios que cuando son aplicados mejoran nuestro nivel técnico. Para dominarlos, recuerde estas sugerencias:

- Demasiadas preguntas pueden hacer retroceder al objetivo. Acosarle con una sarta de preguntas sólo servirá para que se cierre en banda. Recuerde que una conversación consiste en dar y tomar. Tiene que preguntar, pero también tiene que dar algo para que el objetivo se sienta cómodo.
- Si pregunta demasiado poco puede hacer que el objetivo se incomode. ¿Alguna vez se ha encontrado en una conversación llena de "silencios incómodos"? No es una sensación agradable, ¿verdad? No dé por sentado que su objetivo es un gran conversador con ganas de hablar. Debe hacer que la conversación sea una experiencia amena.
- Haga las preguntas una a una. El capítulo 5 explica los desbordamientos de búfer de la mente, pero en este momento no debe "desbordar" a su objetivo. Simplemente busca recopilar información y formar un perfil. Para hacerlo, no puede parecer demasiado ansioso ni desinteresado.

Como puede comprobar, las maniobras de obtención de información son un proceso con un equilibrio delicado. Mucho, poco, demasiado, insuficiente; cualquiera de estas situaciones arruinaría sus opciones.

Esos principios pueden ayudarle a dominar esta habilidad. Intente lo siguiente: imagine la conversación como un embudo en el que en la parte superior están los elementos amplios y "neutrales" y en la parte inferior está el final, estrecho y directo. Empiece formulando preguntas muy neutrales a su objetivo y reúna algo de información a partir de ellas. Aporte algo a la conversación (recuerde que debe dar y tomar) y después pase a realizar preguntas más abiertas. Si es necesario, formule algunas preguntas cerradas para dirigir al objetivo hacia donde desea y, si encaja con la situación, termine realizando preguntas muy directas según vaya llegando al final del embudo. Lo que saldrá por el extremo de ese embudo será un río de información.

Piense en el ejemplo que vimos previamente en este capítulo del encuentro que planeé con un objetivo en la reunión de la cámara de comercio. Mi meta era recabar cualquier tipo de información que me pudiera conducir a una brecha de seguridad.

Empecé la conversación con una pregunta muy neutral: "Qué, ¿huyendo de los buitres?". Esta pregunta sirvió para romper el hielo y, al utilizar el sentido del humor, tendió un puente para situarnos en la misma onda de pensamiento. Le hice algunas preguntas neutrales más y le ofrecí mi tarjeta de visita mientras le preguntaba a qué se dedicaba. De este modo, enlacé suavemente con las preguntas abiertas.

La clave estaba en la pequeña sesión de recopilación de información que llevé a cabo previamente utilizando preguntas cerradas o preguntas de conocimiento asumido. Después de que me explicara sus nuevas adquisiciones de software contable y actualizaciones de redes decidí ir a por todas. Sabía que utilizaban el sistema RFID porque había examinado el edificio, pero no sabía que el objetivo iba a llegar tan lejos como para describir la tarjeta y enseñarme la suya.

Aquí es donde entraron en juego las preguntas directas: preguntándole qué tipo de seguridad utilizaba su empresa. Cuando realicé este tipo de pregunta nuestro nivel de compenetración y confianza mutua era tan alto que probablemente hubiera contestado a cualquier pregunta que le hubiera hecho.

Comprender cómo comunicarse con la gente es una habilidad fundamental. Hay que saber adaptarse y ajustar la conversación al entorno y a la situación. Es vital construir un mínimo de confianza rápidamente. Sin esa compenetración es probable que la conversación se frustre.

Otros factores importantes son conseguir que su estilo de comunicación, las preguntas formuladas y su forma de hablar encajen con su pretexto. La clave del éxito es saber hacer preguntas que fuercen una respuesta, pero si estas técnicas y esas preguntas no encajan con su pretexto, la maniobra fracasará.

Resumen

Este capítulo ha explicado algunos de los puntos más importantes del libro. Puntos que al ser aplicados pueden cambiar sus habilidades como ingeniero social y como comunicador. Saber cómo formular la pregunta adecuada con el tono adecuado y en la forma correcta abre muchas opciones. En este concepto reside la diferencia entre el éxito y el fracaso. Las primeras impresiones se basan, sobre todo, en la vista, pero lo primero que diga también es fundamental. Dominar las maniobras de obtención de información prácticamente le garantiza el éxito y le proporciona una base sólida donde apoyar cualquier pretexto que decida utilizar.

A lo largo del capítulo he mencionado el poder del pretexto. Éste es otro punto que se debe dominar. Pero ¿cómo conseguirlo? Para responder esta pregunta, debe aprender qué es el pretexto, como se explica en el capítulo 4.

4. El pretexto: cómo convertirse en otra persona

La clave en cualquier relación es la honestidad. Si consigue fingirla, tendrá éxito.
Richard Jeni

A todos nos gustaría ser otra persona de vez en cuando. Qué diablos, a mí me encantaría estar más delgado y ser un poco más guapo. Aunque la medicina todavía no ha inventado una pastilla que haga esto posible, existe una solución al dilema: el "pretexto".

¿Qué es el pretexto? Algunas personas dirán que es simplemente un papel o una mentira que se representa durante una acción de ingeniería social, pero ésta es una definición muy limitada. Es más adecuado definir el pretexto como la historia, vestimenta, aspecto, personalidad y actitud de fondo que crean el personaje que se interpretará durante una auditoría. Engloba todo lo que pueda imaginar sobre lo que esa persona es. Cuanto más sólido y más simple sea el pretexto, más creíble resultará.

Desde la llegada de Internet, los usos malintencionados del pretexto han ido en aumento. En una ocasión, vi una camiseta en la que se podía leer: "Internet: el lugar donde los hombres son hombres, las mujeres son hombres y los niños son agentes

del FBI esperando para cazarte". Además de ser una frase bastante graciosa, tiene parte de verdad. En Internet puede ser cualquier persona que quiera. Los *hackers* llevan años aprovechándose de esta habilidad y no sólo en Internet.

En ingeniería social, a menudo, es obligatorio representar un papel o convertirse en otra persona para alcanzar la meta. Puede que yo, Chris Hadnagy, no tenga el mismo tirón que el técnico del servicio de asistencia o que el director general de una gran empresa de importaciones. Cuando se presenta la ocasión, es importante disponer de las habilidades necesarias para representar el pretexto. En una discusión que mantuve sobre este tema con el reputado ingeniero social Chris Nickerson, dijo algo que llamó mi atención.

Nickerson afirmó que el pretexto no consiste en interpretar un papel. Dijo que no consistía en vivir una mentira, sino en convertirse realmente en esa persona. Hay que transformarse por completo en la persona que se está retratando. Su forma de andar, su forma de hablar, su lenguaje corporal: hay que convertirse en ella. Estoy de acuerdo con esta idea. En muchas ocasiones, las películas que consideramos "las mejores que hemos visto jamás" son aquéllas en las que los actores nos cautivan con su papel de tal forma que nos resulta imposible separarlos de sus personajes.

Comprobé este hecho muchos años atrás cuando fui con mi mujer a ver una película de Brad Pitt llamada *Leyendas de pasión*. En esta película, Pitt era un idiota egoísta, un espíritu atormentado que tomaba algunas malas decisiones. Interpretó tan bien este papel que mi mujer odió literalmente al actor durante unos años. En eso consiste lograr un buen pretexto.

El problema es que hay quienes consideran que el pretexto es simplemente disfrazarse. El disfraz puede ayudar, pero el pretexto es una ciencia. En cierto modo, su personaje va a representarle de un modo completamente distinto a quien es en realidad. Para lograrlo, debe tener una idea clara de lo que es el pretexto. Entonces podrá planear y desarrollar sus pretextos a la perfección. Podrá darles los toques finales. En este capítulo, encontrará en primer lugar una explicación de lo que es el pretexto y después un estudio de cómo utilizarlo. Por último, se examinan algunas historias que muestran cómo llevar a cabo el pretexto de forma efectiva.

¿Qué es el pretexto?

El pretexto se define como el acto de crear un escenario inventado para incitar al objetivo a que proporcione cierta información o a que realice cierta acción. Es más que inventar una mentira; en algunos casos puede consistir en crear una identidad completamente nueva y utilizarla para manipular la obtención de in-

formación. Los auditores profesionales pueden utilizarlo para hacerse pasar por personas con ciertos trabajos que ellos mismos nunca han realizado. El pretexto no es una solución global única. Un ingeniero social debe desarrollar muchos a lo largo de su carrera. Todos tendrán una cosa en común: la investigación. Una buena técnica de recopilación de información es fundamental. Por ejemplo, imitar a la perfección a un técnico del servicio de asistencia es inútil si su objetivo no utiliza este tipo de servicio externo.

El pretexto también se utiliza en otras áreas de la vida. Comerciales, oradores públicos, videntes, expertos en programación neurolingüística, incluso médicos, abogados y terapeutas también tienen que utilizar a veces algún tipo de pretexto. Todos ellos tienen que crear situaciones en las que la gente se sienta cómoda facilitando información que normalmente no revelarían. La diferencia entre los ingenieros sociales y el resto está en las metas perseguidas. El ingeniero social debe vivir ese personaje durante un tiempo, no simplemente interpretar un papel.

Mientras dure la auditoría, debe seguir metido en el personaje. Yo, como muchos de mis colegas, consigo hacerlo. Algunos siguen en el personaje incluso fuera de las "horas de trabajo". Cada vez que lo necesite, debe convertirse en el pretexto que ha preparado. Muchos profesionales crean cuentas *on-line*, de correo electrónico y en medios sociales para dar cobertura a sus pretextos.

En cierta ocasión, entrevisté sobre este tema al icono radiofónico Tom Mischke para un *podcast* del que formo parte (alojado en `www.social-engineer.org/episode-002-pretexting-not-just-for-social-engineers/`). Los presentadores de radio deben ser muy buenos creando pretextos porque constantemente deben tener la habilidad para facilitar a sus oyentes sólo la información que desean. Tom era tan bueno en esto que muchos oyentes consideraban que le "conocían" como a un amigo. Recibía invitaciones de boda, le invitaban a cumpleaños e incluso a nacimientos. ¿Cómo conseguía Tom elaborar este tipo de pretexto tan asombroso?

La respuesta es: la práctica. Él recomienda mucha práctica. Me comentó que él planeaba sus "actuaciones" y después las ensayaba: hablaba con la voz que iba a usar, se sentaba y se vestía como su personaje. La práctica es exactamente lo que hace bueno un pretexto.

Un aspecto importante que debe ser recordado es que la calidad del pretexto está directamente relacionada con la calidad de la información obtenida. Cuanta más, mejor y cuanto más relevante sea la información reunida, más rápidamente se desarrollará el pretexto y tendrá éxito. Por ejemplo, el clásico pretexto de ser un técnico del servicio de asistencia no funcionará si va a una empresa que tiene su propio servicio interno o que contrata a una pequeña empresa de sólo dos o tres personas. Con la misma naturalidad con la que habla de sí mismo en una conversación, debe aplicar su pretexto.

Para que pueda comprobar cómo utilizar esta habilidad, la siguiente sección explica los principios del pretexto y le muestra cómo aplicarlos para planificar uno consistente.

Los principios y fases de planificación del pretexto

Del mismo modo que con cualquier otra técnica, ciertos principios señalan los pasos hacia la realización de la tarea.El pretexto no es distinto. A continuación, se expone una lista de los principios que pueden utilizarse. Éstos no son los únicos en absoluto; pueden añadirse otros, pero éstos son los que encarnan la esencia del pretexto:

- Cuanto más investigue, más probabilidades tendrá de tener éxito.
- Si involucra sus intereses personales aumentarán sus opciones.
- Practique dialectos y expresiones.
- Haga el esfuerzo de utilizar el teléfono.
- Cuanto más simple sea el pretexto mayores serán las opciones de tener éxito.
- El pretexto debe parecer espontáneo.
- Proporcione al objetivo una conclusión lógica.

Las siguientes secciones explican en detalle cada uno de estos principios.

Cuanto más investigue, más probabilidades tendrá de tener éxito

Este principio se explica por sí solo, pero nunca se advierte lo suficiente: el nivel de éxito está relacionado directamente con el nivel y la profundidad de la investigación. Como se explicó en el capítulo 2, éste es el quid del éxito en ingeniería social. Cuanta más información se posea, más opciones existen de crear un pretexto que funcione. ¿Recuerda la historia que relaté en el capítulo 2, sobre mi mentor Mati Aharoni y cómo convenció a un ejecutivo para que visitara su sitio Web con la "colección de sellos"? A primera vista, el camino lógico a seguir para penetrar en esa empresa habría sido algo que tuviera que ver con las finanzas, el sector

bancario, la recaudación de fondos o algo por el estilo, porque aquella empresa era un banco. Pero cuando Mati fue profundizando en su investigación, comprendió que su pretexto podía ser un coleccionista de sellos. Al averiguar las aficiones del ejecutivo, Mati encontró una vía para penetrar en la empresa. Y funcionó.

Muchas veces son estos pequeños detalles los que marcan la diferencia. Recuerde: no hay información irrelevante. Al reunir información, es buena idea buscar historias, elementos o aspectos de naturaleza personal. Utilizar las relaciones personales o sentimentales del objetivo también puede ayudarle a alcanzar su meta. Si averigua que todos los años el director general dona una considerable suma de dinero a un centro de investigación contra el cáncer infantil, puede funcionar muy bien un pretexto que implique la recaudación de fondos para esta causa, por muy cruel que parezca esta idea.

El problema está en que los ingenieros sociales maliciosos utilizan pretextos que se aprovechan de las emociones ajenas sin pensarlo dos veces. Después de los ataques a las torres gemelas de Nueva York, el 11 de septiembre de 2001, muchos *hackers* utilizaron la pérdida de estas personas para recaudar fondos para sí mismos a través de sitios Web y correos electrónicos que enviaban a los ordenadores de sus víctimas haciéndose pasar por recaudadores de fondos y obteniendo dinero de personas generosas. Después de los terremotos de Chile y Haití en 2010, ocurrió lo mismo. Ingenieros sociales maliciosos crearon sitios Web que supuestamente proporcionaban información sísmica o sobre las víctimas de los terremotos. Estos sitios escondían código malicioso que pirateó los ordenadores de la gente.

Esta tendencia se hace todavía más evidente justo después de la muerte de un cantante o actor famoso. Los genios del posicionamiento en buscadores y del *marketing* consiguen en cuestión de horas que sus historias lleguen a las primeras posiciones en los motores de búsqueda. Los *hackers* aprovechan el incremento de la atención de los motores de búsqueda y lanzan sitios Web maliciosos que se nutren de ese posicionamiento.

Una vez que atraen a la gente hacia esos sitios Web, le roban información o la infectan con algún virus.

El hecho de que exista gente que saque provecho de la desgracia ajena es una triste realidad de este mundo y uno de esos rincones oscuros que, como les anticipé, se abordan en este libro. Como auditor de seguridad puede utilizar los sentimientos de un empleado para mostrarle a una empresa que incluso una persona con buenas intenciones puede engañar a un empleado para obtener acceso a información valiosa relativa al negocio.

Esto ejemplos confirman que cuanto mejor sea la recopilación de información y la investigación, mayores serán las opciones de encontrar detalles para crear un buen pretexto.

Involucre sus intereses personales para aumentar sus opciones

Involucrar sus intereses personales puede parecer muy simple, pero es muy útil para convencer al objetivo de su credibilidad. Nada destruye más rápido la compenetración y la confianza que una persona que afirma tener conocimientos sobre un tema y después no cumple las expectativas. Por ejemplo, si nunca ha visto un cuarto de servidores y nunca ha desmontado un ordenador, representar el papel de un técnico no dará resultado. Incluir en su pretexto temas y actividades que le interesan le dará mucho de qué hablar y demostrará inteligencia y confianza.

La confianza juega un papel muy importante en que el objetivo le crea. Algunos pretextos requieren más conocimientos que otros para resultar convincentes (por ejemplo, un coleccionista de sellos en oposición a un investigador nuclear), por lo que, de nuevo, la investigación es la clave. En ocasiones, el pretexto es tan sencillo que obtendrá el conocimiento suficiente leyendo un libro o unos cuantos sitios Web.

Independientemente del método que utilice para ampliar sus conocimientos, es importante investigar los temas que le interesen personalmente. Cuando descubra un tema o materia que conozca bien o con el que se sienta cómodo conversando, analice si ese planteamiento puede funcionar.

El doctor Tom G. Stevens dice: "Es importante recordar que la confianza en uno mismo siempre está relacionada con la tarea y con la situación. Tenemos diferentes niveles de confianza en situaciones diferentes". Esta afirmación es muy importante porque la confianza se relaciona directamente con el modo en que otros le ven. La confianza (siempre que no sea excesiva) genera seguridad y compenetración y hace que la gente se sienta cómoda. Es importante encontrar un camino hacia sus objetivos que le dé la oportunidad de hablar de temas con los que se sienta a gusto y de los que pueda hablar con seguridad.

En 1957, el psicólogo Leon Festinger desarrolló la teoría de la disonancia cognitiva. Esta teoría establece que la gente tiene tendencia a buscar la consistencia y coherencia entre sus creencias, opiniones y en general en todas sus actitudes o procesos cognitivos.

Cuando existe una inconsistencia entre actitudes o comportamientos, debe haber un cambio para eliminar la disonancia. El doctor Festinger estableció lo dos factores que afectan a la intensidad de la disonancia:

- La cantidad de creencias disonantes.
- La importancia de cada creencia.

También estableció que existen tres modos de eliminar la disonancia (y esto es importante para el ingeniero social):

- Reducir la importancia de las creencias disonantes.
- Incluir más creencias consonantes que superen a las disonantes.
- Cambiar las creencias disonantes para que dejen de ser inconsistentes.

¿Cómo podemos utilizar esta información? Interpretar un pretexto sin confianza, cuando ese pretexto exige que esté seguro de sí mismo, provoca disonancia automáticamente. Esta disonancia dispara las alarmas y se crean barreras a la compenetración, la confianza del objetivo y la capacidad para avanzar. Estas barreras afectan a la conducta del objetivo que intentará entonces equilibrar sus sentimientos disonantes, eliminando cualquier opción de que su pretexto funcione.

Uno de los métodos para contrarrestar este efecto es incluir más creencias consonantes hasta que superen a las disonantes. ¿Qué espera el objetivo de su pretexto? Saber esto le permitirá llenar su mente de emociones, acciones, palabras y actitudes que crearán un sistema de creencias que superará los sentimientos que provocan duda.

Por supuesto, un ingeniero social habilidoso puede cambiar las creencias disonantes para que dejen de ser inconsistentes. Aunque es más compleja, es una habilidad poderosa. Puede que su aspecto no encaje con la imagen que el objetivo tiene de su pretexto. Si recuerda la serie de televisión *Médico precoz*, el problema del médico, Doogie Howser, era que su "pretexto" de ser un gran médico no encajaba porque era demasiado joven. Aquello era una creencia disonante, pero sus conocimientos de medicina y sus acciones casi siempre pasaban a formar parte de las creencias consonantes de sus "objetivos". Al igual que en este ejemplo, el ingeniero social puede alinear su pretexto con las creencias de sus objetivos a través de sus acciones, actitudes y, sobretodo, con su conocimiento del pretexto.

Presencié un ejemplo de este tema recientemente, en la conferencia Defcon 18. Formaba parte del equipo que creó el Social Engineering CTF, un concurso de ingeniería social, para Defcon. Vimos que muchos participantes utilizaban el pretexto de un empleado interno. Cuando se les planteaba una pregunta como: "¿Cuál es tu número identificativo de empleado?", los más inexpertos se ponían nerviosos y no sabían qué responder, mientras que un concursante habilidoso conseguía alinear esas creencias disonantes con el objetivo.

Simplemente dando un número que había encontrado en Internet o utilizando cualquier otro método era capaz de convencer al objetivo de que esa información no era necesaria, consiguiendo de este modo alinear al objetivo con sus creencias.

Éstas son respuestas muy técnicas a un problema muy sencillo, pero debe comprender que sólo podrá llevar la representación de su papel hasta cierto punto. Elija su camino sabiamente.

Practique dialectos y expresiones

Aprender a hablar dialectos diferentes no es algo que se deba tomar a la ligera. Dependiendo de su lugar de origen puede llevarle bastante tiempo hablar otro dialecto o con un acento distinto. Poner acento del sur o asiático, por ejemplo, puede ser muy difícil, si no imposible. En cierta ocasión, en unas clases que impartía una organización de ventas internacionales, dieron unas estadísticas que señalaban que el 70 por 100 de los estadounidenses prefiere escuchar a gente con acento británico. No estoy seguro de si ese dato es cierto, pero puedo decir que a mí me gusta ese acento. Después de la clase, escuché a varias personas intentando imitar el acento británico con resultados terribles. Un buen amigo de Reino Unido, Jon, se enfada mucho cuando escucha a estadounidenses utilizar frases de Mary Poppins para imitar el acento británico. Si hubiera escuchado a este grupo se habría puesto muy furioso.

Lo que esa clase me enseñó es que, aunque unas estadísticas digan que en ventas un acento es mejor que otro o simplemente porque esté trabajando en un lugar lejano, eso no significa que pueda poner fácilmente el acento local. Ante la duda, déjelo. Si no puede imitar el acento a la perfección, si no resulta fluido y natural, mejor no lo intente. Los actores utilizan preparadores y sesiones de aprendizaje para hablar con claridad en el acento del papel que tienen que representar. El actor Christian Bale es galés, pero es muy difícil adivinarlo escuchándolo hablar. No suena británico en la mayoría de sus películas. Por su parte, la actriz Gwyneth Paltrow logró un acento británico muy convincente en la película *Shakespeare in Love*.

La mayoría de actores tienen preparadores que les ayudan a conseguir el acento que buscan. La gran mayoría de ingenieros sociales no pueden permitirse un preparador, pero existen varias publicaciones que pueden ayudarle a aprender los conceptos básicos para lograr un acento, como el libro de Eveline Machlin. Aunque es un libro antiguo, contiene muchos buenos consejos:

- Escuche muestras del acento nativo que quiere aprender. Libros como el de Eveline Machlin contienen cintas con acentos para escuchar.
- Intente hablar al mismo tiempo que la grabación que está escuchando para comprobar si suena como esa persona.
- Cuando se sienta seguro, grabe su propia voz para poder corregir errores.
- Invente una situación y practique el acento con un ayudante.
- Utilice el acento en público para comprobar si la gente se lo cree.

Existen innumerables acentos y dialectos. A mí me resulta útil escribir fonéticamente las frases que tengo que utilizar. Esto me permite practicar leyéndolas y meterme las ideas en la cabeza para que mi acento resulte más natural.

Estos consejos le pueden ayudar a utilizar otro dialecto con fluidez.

Aunque no consiga hablar con otro acento, puede conseguir buenos resultados si aprende expresiones que se utilicen en la zona en la que está trabajando. Un método es pasar algún tiempo en lugares públicos escuchando a la gente hablar entre sí. Un sitio muy bueno para esto es un restaurante o un centro comercial o cualquier otro lugar donde encuentre grupos de personas sentadas charlando. Preste atención a las frases y a ciertas palabras clave.

Si percibe que se utilizan en varias conversaciones, busque el modo de introducirlas en su pretexto para ganar credibilidad. Una vez más, este ejercicio necesita investigación y práctica.

Haga el esfuerzo de utilizar el teléfono

En los últimos años, Internet se ha convertido en la fuerza dominante de ciertos aspectos más "impersonales" de la ingeniería social, mientras que en el pasado el teléfono era una parte integrante de la misma. Debido a este cambio, muchos profesionales no se toman la molestia de utilizar el teléfono, desestimando su utilidad.

Este punto viene a demostrar que el teléfono es todavía una de las herramientas más poderosas del ingeniero social y no debe limitarse su utilización debido al carácter más impersonal de Internet.

A menudo, cuando se planea un ataque telefónico, debe cambiarse de mentalidad, porque utilizar Internet puede parecer más sencillo. Tenga en cuenta que debe poner el mismo esfuerzo, la misma profundidad en la investigación y en la recopilación de información y, lo que es más importante, la misma cantidad de práctica en sus ataques telefónicos. En cierta ocasión, me encontraba con un grupo que iba a poner en práctica unas presentaciones telefónicas. Señalamos los métodos apropiados, el tono y la velocidad de la voz y las palabras que debían utilizarse. Escribimos un esquema de guión (trataremos este punto enseguida) y comenzamos la sesión. La primera persona hizo la llamada, habló con alguien y se hizo un lío en las primeras líneas y lo echó todo a perder. Debido a la vergüenza y al miedo, colgó a la persona con la que estaba hablando. Hay una buena lección que aprender aquí: la persona al otro lado del teléfono no sabe lo que va a decir el otro, por lo que en realidad no hay nada que "echar a perder". Las prácticas pueden ayudarle a aprender a manejar el "terreno desconocido" en el que se cae cuando accidentalmente se altera alguna parte del guión dejándole desorientado.

Si no tiene la suerte de contar con un grupo con el que practicar y poner a punto estas habilidades, entonces tiene que ser creativo. Prueba a llamar a familiares o amigos para comprobar lo lejos que puede llegar manipulándolos. Otro modo de practicar es grabar su voz como si estuviera hablando por teléfono para comprobar después cómo suena.

Personalmente, opino que preparar un guión es muy importante. Aquí tiene un ejemplo: imagine que tiene que llamar a su compañía telefónica u otra empresa de servicios. Puede que haya habido un problema con la factura o que se haya estropeado el servicio otra vez y quiere presentar una queja. Después de explicar su situación al agente comercial, diciéndole lo disgustado y decepcionado que está, el agente no hace absolutamente nada por usted y le dice: "En la empresa X siempre nos comprometemos a ofrecer un servicio excelente; ¿tiene alguna otra pregunta?". Si la voz monótona del otro lado del teléfono hubiera pensado por un momento lo que estaba diciendo, se habría dado cuenta de lo tonta que era la pregunta, ¿verdad? Esto es lo que pasa cuando se tiene un guión escrito en lugar de un esquema. Un esquema le deja espacio para la "libertad creativa", le permite moverse por la conversación sin preocuparse por qué será lo que "debe" decir después.

Utilizar el teléfono para consolidar su pretexto es una de las vías de acceso más rápidas a su objetivo. El teléfono le permite "parodiar" o imitar prácticamente cualquier cosa. Considere este ejemplo: si quiero llamarle y aparentar que estoy en una oficina bulliciosa para apoyar mi pretexto sólo tengo que utilizar la pista de audio de Thriving Office (`www.thrivingoffice.com/`). Este sitio Web ofrece una pista llamada "ajetreado" y otra llamada "muy ajetreado". Esto es lo que comentan sus creadores: "Este valioso CD, que contiene los sonidos que la gente espera escuchar en las oficinas de una empresa consolidada, proporciona credibilidad instantánea. ¡Es sencillo, efectivo y está garantizado!".

Esa frase por sí sola es muy valiosa en ingeniería social: contiene lo que "la gente espera escuchar" en las oficinas de una empresa consolidada. Puede ver que el CD está pensado para satisfacer las expectativas y proporcionar credibilidad (al menos, en la mente del objetivo) generando confianza automáticamente.

Además, falsificar la información del identificador de llamadas es relativamente sencillo. Con servicios como SpoofCard (`www.spoofcard.com`) o utilizando soluciones caseras, se puede hacer creer al objetivo que se está llamando desde una empresa concreta, desde la Casa Blanca o desde su banco. Con este servicio, se puede falsificar el número desde el que está llamando desde cualquier parte del mundo.

El teléfono es un arma mortífera para un ingeniero social; desarrollar el hábito de practicar con él y tratarlo con absoluto respeto ampliará sus recursos para elaborar sus pretextos. Ya que el teléfono es un arma tan letal que no ha perdido su efectividad, debe dedicarle el esfuerzo y el tiempo que merece.

Cuanto más simple sea el pretexto mayores serán las opciones de tener éxito

"Cuanto más sencillo, mejor". Este principio no puede recordarse lo suficiente. Si el pretexto tiene tantos detalles complicados que olvidar uno supondría el fracaso de la acción, ésta probablemente fracasará. Mantener la historia, los hechos y los detalles sencillos ayuda a generar credibilidad.

El doctor Paul Ekman, un renombrado psicólogo e investigador en el campo del engaño humano, escribió un artículo 1993 junto a otros autores titulado "Lies That Fail" (Mentiras que fracasan). En ese artículo decía:

No siempre hay tiempo para preparar la línea de acción a seguir, para ensayarla y memorizarla. Incluso cuando ha habido un amplio conocimiento previo y se ha ideado cuidadosamente una línea falsa, el mentiroso puede no ser lo suficientemente listo como para anticipar todas las preguntas que se le pueden formular y haber pensado cuáles serían sus respuestas. Puede que ser listo tampoco sea suficiente, porque los cambios inesperados en las circunstancias pueden traicionar una línea que de otra forma sería efectiva. E, incluso cuando no se ven obligados por las circunstancias a cambiarlas, algunos mentirosos tienen problemas para recordar las líneas que habían preparado previamente, por lo que esas nuevas preguntas no pueden contestarse rápida y consistentemente.

Esta idea tan importante explica claramente por qué la sencillez es la mejor opción. Intentar recordar un pretexto es casi imposible si es tan complicado que puede venirse abajo por un simple error. El pretexto debe ser natural y fluido. Debe ser fácil de recordar y, si le resulta natural, entonces recordar los hechos o las líneas seguidas previamente no será tarea complicada. Para ilustrar lo importante que es recordar los pequeños detalles, me gustaría contarle una historia. Hace mucho tiempo probé suerte en el campo de las ventas. Me asignaron un supervisor para enseñarme el funcionamiento del trabajo. Puedo recordar la primera visita que hicimos juntos. Llegamos a la casa y antes de salir del coche comprobó la información y me dijo: "Recuerda, Becky Smith ha enviado una solicitud de cobertura adicional del seguro. Vamos a presentar la póliza X. Mira y aprende".

En los primeros tres minutos de la visita, la llamó Beth y Betty. Cada vez que se confundía con el nombre, podía observar cómo ella cambiaba de expresión y decía tranquilamente "Becky". Tuve la impresión de que, aunque estuviéramos regalando lingotes de oro, ella nos habría rechazado. Estaba tan desmotivada por que él no pudiera recordar su nombre, que no tenía interés por escuchar nada.

Esta situación demuestra claramente la importancia de ser exactos con los datos sencillos. Además de recordarlos, es igual de importante que contengan pocos detalles. Un pretexto simple permite que la historia crezca y que el objetivo utilice

su imaginación para completarla. No intente hacer su pretexto muy elaborado y, sobre todo, recuerde los pequeños detalles que marcarán la diferencia en el modo en que la gente percibe el pretexto.

Por otra parte, aquí tiene un dato interesante: una táctica popular entre los delincuentes y los estafadores es cometer algunos errores a propósito. La idea es que "nadie es perfecto" y algún que otro error hace que la gente se relaje. Tenga cuidado eligiendo los errores que va a cometer si decide utilizar esta táctica porque complica su pretexto, pero hace que la conversación resulte más natural. Utilice esta técnica con moderación e independientemente de cómo decida proceder, hágalo con sencillez.

Permítame enlazar todos estos conceptos con algunos ejemplos que he utilizado o he visto utilizar en algunas auditorías. Después de un gran trabajo de obtención de información al teléfono, un ingeniero social anónimo consiguió el nombre de la empresa de recogida de basuras. Hizo unas sencillas búsquedas en Internet y consiguió un logo imprimible. Existen docenas de tiendas físicas y en Internet que imprimen camisetas o gorras con cualquier logo.

Preparó el material y encargó una camisa y una gorra con el logo de la empresa de recogida de basuras. Unos días después apareció frente a la cabina de seguridad de la empresa objetivo vestido con la ropa impresa.

Dijo: "Hola, soy Joe de la empresa X. Nos han llamado del departamento de compras para que viniera alguien a comprobar un contenedor estropeado en la parte trasera. La recogida es mañana y si el contenedor no se puede reparar haré que manden uno nuevo. Pero tengo que ir a comprobarlo".

Sin pestañear, el guardia de seguridad dijo: "De acuerdo, tiene que llevar esta tarjeta de identificación para pasar. Entre por aquí y conduzca hasta la parte de atrás. Allí encontrará los contenedores".

El auditor había conseguido un pase que le permitía llevar a cabo una larga y minuciosa inspección en un contenedor pero decidió sacarle el máximo partido a la situación y fue a por todas con la siguiente frase. Mirando su carpeta, dijo: "La nota dice que no es uno de los contenedores de comida, sino uno de los que contienen papeles y deshechos de oficina. ¿En qué bloque están ésos?".

"Ah, vaya por donde le he dicho y los encontrará en la tercera plataforma", contestó el guardia.

"Gracias", dijo Joe.

Un pretexto sencillo, respaldado por el vestuario y alguna "herramienta" (como la carpeta) y un argumento fácil de recordar. La sencillez y ausencia de detalles hicieron este pretexto más creíble, por eso funcionó.

Otro pretexto muy utilizado es el del técnico de asistencia. Para llevarlo a cabo sólo hace falta vestirse con un polo y unos pantalones caqui y llevar una pequeña bolsa de herramientas para ordenadores. Muchos profesionales deciden utilizar

esta táctica porque al técnico de asistencia se le suele dar acceso a cualquier parte sin supervisión. Se aplica la misma regla: desarrollar un argumento simple ayudará a que este pretexto resulte real y creíble.

El pretexto debe parecer espontáneo

Conseguir que el pretexto parezca espontáneo nos lleva de vuelta al punto de utilizar un esquema en lugar de un guión. El esquema siempre permitirá más libertad de movimientos mientras que el guión puede provocar que el ingeniero social suene demasiado robótico. También implica que se utilicen elementos o historias que le interesen personalmente. Si cada vez que alguien le haga una pregunta tiene que pararse a pensar diciendo cosas como "Hummm..." y después no es capaz de dar una respuesta inteligente, arruinará su credibilidad. Por supuesto, mucha gente piensa antes de contestar, esto no consiste en dar una respuesta en un segundo, sino en tener una respuesta o una razón para no tener una respuesta. Por ejemplo, en una llamada que hice me preguntaron un dato que desconocía. Simplemente dije: "Un momento, voy a buscarlo". Me aparté un poco e hice como si le estuviera gritando a un compañero: "Jill, ¿puedes pedirle a Bill que me traiga el pedido de la cuenta X? Gracias".

Después, mientras "Jill" me conseguía el documento, pude sonsacarle al objetivo la información que quería y el documento no volvió a mencionarse.

He confeccionado una pequeña lista con las maneras de poder practicar la espontaneidad:

- **No piense en sus propios sentimientos:** Éste es un buen punto porque muchas veces, durante un pretexto, si piensa demasiado pueden mezclarse muchas emociones, provocando miedo, nerviosismo o ansiedad, lo que le llevaría al fracaso. Por otra parte, puede que no sienta nerviosismo o miedo, pero puede sentirse sobreexcitado y cometer muchos errores.
- **No se tome a sí mismo demasiado en serio:** Por supuesto, éste es un consejo muy bueno para la vida en general, pero aquí tiene mucho sentido. Como ingeniero social, tiene un trabajo serio; la seguridad es un asunto serio. Pero si no es capaz de reírse de sus errores puede bloquearse o ponerse tan nervioso que no pueda sobreponerse a un pequeño bache en el camino. No estoy sugiriendo que se tome la seguridad como una broma. Sin embargo, si considera que un error potencial sería la cumbre del fracaso en la vida, la presión que crea puede provocar que suceda precisamente lo que más teme. Los pequeños fallos pueden conducir a un gran éxito si sabe cómo arreglárselas.

- **Aprenda a identificar lo que es importante:** Me gusta expresar este concepto como: "Sal de tu mente y entra en el mundo". Éste es un gran consejo. Un ingeniero social puede estar planeando lo que va a ocurrir tres pasos más adelante y mientras tanto pasar por alto un detalle importante que haga que el pretexto fracase. Identifique rápidamente la información y los elementos importantes, ya sea el lenguaje corporal del objetivo, lo que está diciendo, las microexpresiones (véase el capítulo 5 para más información sobre este tema) e integre la información en su vector de ataque.

  También tenga en cuenta que la gente percibe cuándo alguien no está escuchando lo que le están diciendo. Mucha gente perderá interés si considera que no presta atención a la conversación, aunque ésta sea irrelevante. Todo el mundo ha experimentado estar con alguien a quien no parece importarle lo que le dicen. Puede que la persona tenga una buena razón para no estar escuchando, pero aun así es frustrante.

  Haga el esfuerzo de escuchar lo que le dice el objetivo. Preste atención y captará pequeños detalles que pueden ser importantes y llevarle al éxito.

- **Intente acumular experiencia:** Este concepto vuelve a lo que probablemente verá repetido un millón de veces en este libro: la práctica. Acumular experiencia a través de la práctica es clave para que el pretexto funcione. Practique su espontaneidad con la familia, los amigos y con desconocidos sin ninguna meta más que ser espontáneo. Entable conversaciones con la gente pero sin resultar intimidatorio. Pequeñas y sencillas conversaciones pueden ayudarle mucho a sentirse cómodo siendo espontáneo.

Todos estos puntos pueden situarle en una posición ventajosa cuando desarrolle su pretexto. Tener la habilidad de resultar espontáneo es un don. Anteriormente, en este capítulo, mencioné mi entrevista con Tom Mischke, que tiene un interesante punto de vista sobre la espontaneidad. Él dice que quiere provocar la ilusión de ser espontáneo, a base de práctica y preparación. Practica tanto que su pretexto resulta una exhibición espontánea de humor y talento.

Proporcione al objetivo una conclusión lógica

Aunque no lo crea, a la gente le gusta que le digan lo que tiene que hacer. Imagine que va al médico y éste entra, le examina, anota algo en sus libros y le dice: "Muy bien, nos vemos el mes que viene". Esto sería inaceptable. Incluso aunque sean malas noticias, la gente quiere saber cuál es el siguiente paso y qué es lo que tiene que hacer.

Una vez que haya terminado con un objetivo, puede que quiera que realice una acción o puede que ya tenga lo que quería y sólo desee marcharse. En cualquier caso, es importante proporcionarle al objetivo una conclusión lógica para satisfacer sus expectativas. Igual que el doctor que le examina y le manda a casa sin darle instrucciones, si usted entra en una empresa como el técnico de asistencia y después de hacer su trabajo se va sin decir nada, dejará a todo el mundo preguntándose qué ha pasado. Puede que incluso alguien llame a la empresa de servicio técnico para preguntar qué tienen que hacer ahora. Ésta no es la forma correcta de marcharse. Una frase sencilla, como "he comprobado los servidores y he reparado el sistema de archivo; la velocidad aumentará un 22 por 100 en los próximos días", deja en el objetivo la sensación de que ha sido un "dinero bien gastado".

El caso más complejo es cuando el objetivo tiene que realizar alguna acción después de que el auditor se marche. Si la acción es fundamental para completar la auditoría, quizá lo mejor es que intente realizar la acción el propio auditor. Por ejemplo, en la historia comentada en el capítulo 3 sobre mi sesión de recopilación de información en la fiesta de la cámara de comercio, si mi meta es continuar comunicándome con mi objetivo por correo electrónico, podía haber dicho: "Aquí tienes mi tarjeta; ¿puedes mandarme un correo el lunes con más detalles sobre el asunto?". Él podría haberme mandado el correo electrónico, pero también podría haber llegado a la oficina y haberse olvidado completamente de mí, haciendo que toda la acción fracasara. Por eso, sería mejor decir: "Me gustaría que me dieses más información sobre este tema. ¿Qué te parece si te llamo o te mando un correo electrónico el lunes y me cuentas más detalles?".

Lo que esté pidiendo debe cuadrar con su pretexto. Si representa a un técnico de asistencia, no puede dar "órdenes" a la gente de alrededor diciéndoles lo que tienen que hacer. Si es un mensajero, no puede pedir acceso al cuarto de servidores.

Como hemos mencionado anteriormente, puede haber más pasos para perfeccionar un pretexto, pero los que hemos explicado en este capítulo proporcionan una buena base para elaborar un pretexto perfectamente creíble.

Puede que se esté preguntando: "Muy bien, tengo esta lista de principios, ¿y ahora qué?". ¿Cómo puede elaborarse un pretexto creíble, bien estudiado, que suene espontáneo, que sea sencillo, que funcione tanto por teléfono como en persona y que dé los resultados deseados? Continúe leyendo.

Pretextos exitosos

Para aprender a elaborar un pretexto exitoso, preste atención a estas dos historias de ingenieros sociales que utilizaron un pretexto y a cómo los desarrollaron. Finalmente les cogieron, por eso conocemos estas historias.

Ejemplo 1: Stanley Mark Rifkin

A Stanley Mark Rifkin se le atribuye uno de los mayores atracos a un banco de la historia de Estados Unidos (lea un gran artículo sobre él en `www.social-engineer.org/wiki/archives/Hackers/hackers-Mark-Rifkin-Social-Engineer-furtherInfo.htm`). Rifkin era un loco de los ordenadores que tenía un negocio de consultoría informática en su pequeño apartamento. Uno de sus clientes era una empresa que gestionaba los ordenadores del Security Pacific Bank. La sede del banco en Los Ángeles era un edificio de 55 plantas que parecía una fortaleza de granito y cristal. Guardias vestidos de negro deambulaban por el vestíbulo y cámaras ocultas grababan a los clientes mientras hacían sus ingresos y sus retiradas de dinero.

El edificio parecía impenetrable, así que, ¿cómo es posible que Rifkin saliera de él con 10,2 millones de euros sin haber utilizado un arma, sin tocar ni un billete y sin retener a nadie?

Las políticas de transferencia electrónica del banco parecían seguras. Se autorizaban con un código numérico que cambiaba a diario y que sólo se proporcionaba a personal autorizado. El código se anunciaba en una pared del cuarto de seguridad al que sólo tenía acceso "personal autorizado".

Éste es un extracto del artículo mencionado anteriormente:

En octubre de 1978 visitó el banco, donde los empleados le reconocieron rápidamente como un informático que trabajaba para ellos. Bajó en ascensor al almacén donde estaba localizado el cuarto de transferencia electrónica. Como era un joven agradable y amigable, hablando con la gente consiguió que le dejaran entrar en el cuarto donde el código secreto del día estaba anunciado en la pared. Rifkin memorizó el código y se marchó sin levantar sospecha.

Al poco tiempo los empleados del cuarto de transferencias del banco recibieron una llamada de un hombre que se identificó como Mike Hansen, un empleado de la división internacional del banco. El hombre pidió una transferencia rutinaria de fondos a una cuenta de la Irving Trust Company en Nueva York y proporcionó el código secreto para autorizar la transacción. No había nada fuera de lo normal en aquella transferencia y el Security Pacific transfirió el dinero al banco de Nueva York. Lo que no sabían los empleados del banco era que el hombre que decía llamarse Mike Hansen era en realidad Stanley Rifkin, que había utilizado el código de seguridad del banco para robarles 10,2 millones de euros.

Este escenario da mucho que hablar pero de momento, nos centraremos en el pretexto. Piense en los detalles de lo que tuvo que hacer:

- Tuvo que sentirse cómodo y confiado para no levantar sospechas dentro de ese cuarto.
- Necesitaba una historia creíble al llamar para hacer la transferencia y necesitaba los detalles que sostuvieran esa historia.
- Tenía que ser lo suficientemente espontáneo para contestar a las preguntas que podían surgir.
- Tenía que mantener la calma en todo momento para no levantar ninguna sospechas.

Este pretexto tuvo que planificarse meticulosamente, pensando con sumo cuidado en cada detalle. No le cogieron hasta que visitó a un antiguo asociado y su pretexto falló. Cuando le cogieron, mucha gente que le conocía se sorprendió e incluso algunos dijeron cosas como: "Es imposible que sea un ladrón; todo el mundo aprecia a Mark".

Obviamente, su pretexto era sólido. Tenía un plan bien pensado y presumiblemente bien ensayado. Sabía lo que tenía que hacer e interpretó su papel a la perfección. Cuando se enfrentó con extraños, supo interpretar su personaje; su caída llegó cuando estaba con un colega que le conocía. Ese compañero había leído la noticia, ató cabos y denunció a Mark.

Increíblemente, mientras estaba en libertad bajo fianza, Rifkin empezó a planificar un ataque a otro banco utilizando el mismo procedimiento, pero un topo del gobierno le tendió una trampa; le cogieron y pasó ocho años en una prisión federal. Aunque Mark es un "chico malo" se puede aprender mucho sobre el pretexto leyendo su historia. Consiguió que fuera sencillo y utilizó elementos con los que estaba familiarizado para elaborar el argumento.

El plan de Mark era robar el dinero y convertirlo en un producto no rastreable: diamantes. Para conseguirlo, primero tenía que ser un empleado de banco para realizar el robo, después un importante comerciante de diamantes para deshacerse del dinero y, finalmente, vender los diamantes para tener en su bolsillo dinero en efectivo y no rastreable.

Aunque su pretexto no necesitaba disfraces complicados ni patrones de pronunciación especiales, tenía que representar el papel de un empleado de banco, un comprador y un vendedor de diamantes. Cambió de papel cuatro o cinco veces y lo hizo tan bien que consiguió engañar prácticamente a todo el mundo.

Mark sabía quiénes eran sus objetivos y manejó este escenario ejecutando todos los principios explicados anteriormente. Por supuesto, no se puede aprobar lo que hizo, pero su talento para el pretexto es admirable. Si hubiera puesto su talento al servicio de una buena causa, probablemente habría sido un gran actor o vendedor o una importante figura pública.

Ejemplo 2: Hewlett-Packard

En 2006, la revista *Newsweek* publicó un artículo muy interesante (`www.social-engineer.org/resources/book/HP_pretext.htm`). Básicamente, la presidenta de HP, Patricia Dunn, contrató a un equipo de especialistas en seguridad que a su vez contrató a un equipo de investigadores privados que utilizó el pretexto para obtener registros telefónicos. Estos profesionales consiguieron entrar e interpretaron el papel de miembros de la junta de HP y de la prensa. Todo esto se hizo para descubrir una supuesta filtración de información entre las filas de HP.

La señora Dunn quería conseguir los registros telefónicos de los miembros de la junta y de los periodistas (no los registros de las instalaciones de HP, sino los registros de los números de su casa y de su móvil) para verificar su suposición sobre dónde estaba la filtración. El artículo de *Newsweek* dijo:

El 18 de mayo, en la sede de HP en Palo Alto, California, Dunn soltó la bomba en la junta: había encontrado al informador. Según Tom Perkins, un director de HP presente en ese momento, Dunn diseñó el plan de vigilancia y señaló al director culpable, que admitió ser el informador de CNET. El director, cuya identidad no ha sido publicada hasta el momento, pidió disculpas. Después el director, dirigiéndose al resto de compañeros, dijo: "Os habría contado todo esto, ¿por qué no me preguntasteis?". En ese momento le pidieron que abandonara la sala y lo hizo, según Perkins.

Lo más significativo es lo que se menciona después sobre el pretexto:

El caso HP también pone en entredicho las cuestionables tácticas utilizadas por los consultores de seguridad para obtener información personal. HP reconoció, en un correo electrónico enviado a Perkins desde su consultoría externa, que obtuvieron la prueba escrita que necesitaban para relacionar al director-informador con CNET a través de una controvertida práctica llamada "pretexto"; Newsweek consiguió una copia de dicho correo electrónico. Esta práctica, según la Federal Trade Commission (Comisión federal de comercio), utiliza 'motivaciones falsas' para obtener información privada de otra persona: registros telefónicos, números de cuenta bancaria y de tarjetas de crédito, números de la seguridad social, etc.

La forma de operar de estos profesionales, por ejemplo en el caso de una compañía telefónica, es llamar por teléfono y hacerse pasar por un cliente; ya que las empresas casi nunca piden contraseñas, la persona representando el pretexto sólo necesita una dirección de correo, un número de cuenta y resultar convincente con su petición, para obtener los detalles de una cuenta. Según el sitio Web

de la Federal Trade Commission, después venden esta información a individuos que pueden ser desde investigadores privados legítimos, prestamistas, litigantes potenciales o esposas desconfiadas, hasta quienes pretenden robar o conseguir saldo de forma fraudulenta. El pretexto, según el sitio Web de la Comisión, "va contra la ley". La Comisión federal y muchos fiscales generales estatales han tomado medidas legales contra estos profesionales por violar supuestamente las leyes estatales y federales sobre fraude, falsa identidad y competencia desleal. Uno de los directores de HP es Larry Babbio, el presidente de Verizon, que tiene archivadas varias acciones contra estos profesionales.

Si está interesado en examinarla, puede encontrar la ley de protección y privacidad de registros telefónicos en: `http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h4709enr.txt.pdf`.

El resultado final fue que se presentaron cargos penales no sólo contra Dunn sino también contra los consultores que contrató. Puede que se esté preguntando: "¿Cómo es esto posible teniendo en cuenta que fueron contratados para realizar estas pruebas?".

Para poder ayudarle a contestar este pregunta, eche un vistazo a los métodos que utilizaron y a la información que obtuvieron. Los consultores consiguieron nombres, direcciones, números de la Seguridad Social, registros de llamadas, registros de facturas telefónicas y otros datos de los miembros de la junta de HP y de los periodistas. Incluso utilizaron el número de la Seguridad Social de un periodista para crear una cuenta *on-line* y obtener registros de sus llamadas personales.

La página 32 de un documento confidencial de Hewlett-Packard a su departamento legal (`www.social-engineer.org/resources/book/20061004hewlett6.pdf`) contiene un comunicado de Tom Perkins a los miembros de la junta de HP que indica en más detalle los pretextos que se llevaron a cabo. Algunas tácticas que se utilizaron fueron:

- Se hicieron pasar por trabajadores del operador telefónico para obtener ilegalmente registros de llamadas.
- Se suplantaron las identidades de los directivos investigados para conseguir registros de llamadas personales.
- Se crearon cuentas *on-line* con los operadores utilizando datos obtenidos ilegalmente como nombres, números de la Seguridad Social y otra información, para acceder a sus registros de llamadas.

El 11 de septiembre de 2006, el House of Representatives Committee on Energy and Commerce (Comité de energía y comercio de la cámara de representantes) de Estados Unidos envió una carta a la señora Dunn (puede ver

una copia de esta carta en www.social-engineer.org/resources/book/20061004hewlett6.pdf) solicitándole la información que había obtenido. En su petición, enumeraron la información de la siguiente manera:

- Todos los números de teléfono publicados y no publicados.
- Facturas de tarjetas de crédito.
- Información de direcciones y nombres de clientes.
- Facturas de servicios.
- Números de buscapersonas.
- Números de teléfonos móviles.
- Números de la Seguridad Social.
- Informes de crédito.
- Información de apartados de correos.
- Información de cuentas bancarias.
- Información de activos.
- Otra información de clientes.

Toda esta información se obtuvo deambulando por una zona muy ambigua de la ingeniería social: ¿lo que hicieron fue ético y moral, independientemente de que se les contratara para ello? Muchos profesionales nunca llegarían tan lejos. La lección que se puede aprender de este caso tan serio es que deben imitarse los métodos y la forma de pensar de los ingenieros sociales maliciosos, pero nunca se debe llegar completamente a su nivel. El problema con estos consultores fue que estaban autorizados para realizar esa auditoría en Hewlett-Packard. No estaban autorizados a auditar a empresas como AT&T, Verizon, etc. Cuando vaya a llevar a cabo un pretexto, debe planificar para conocer los límites legales y las líneas que no debe cruzar.

La historia de HP serviría para realizar un discusión más profunda sobre políticas, contratos y para determinar lo que puede ofrecer como auditor, pero estos temas no forman parte de este capítulo. Utilizando los principios señalados anteriormente, podrá tomar decisiones que le mantendrán alejado de los problemas.

El peligro del pretexto malicioso es la amenaza del robo de identidad, lo que lo convierte en una parte muy importante de las pruebas de seguridad. Comprobar y verificar que los empleados de sus clientes no caen en los métodos de los ingenieros sociales maliciosos le será de gran ayuda para protegerse de un ataque.

Mantenerse en terreno legal

En 2005, la revista *Private Investigator* (Investigador privado) realizó una entrevista a Joel Winston, subdirector de la Federal Trade Commision (Comisión federal de comercio), división de prácticas financieras. Su despacho se encarga de regular y controlar la utilización del pretexto (vea una copia de este valioso artículo en `www.social-engineer.org/resources/book/ftc_article.htm`).

Aquí tiene algunos puntos clave de esta entrevista:

- Según la Comisión federal de comercio, el pretexto es la obtención de "cualquier información" (no sólo información financiera) de un banco o un consumidor, utilizando para ello el fraude, el engaño o preguntas capciosas.
- Utilizar información obtenida previamente para confirmar que alguna persona o entidad es un objetivo, es legal según la definición del pretexto de la Comisión, siempre y cuando esos datos no se utilicen para obtener información de una institución financiera.
- Obtener registros de teléfonos móviles o de llamadas telefónicas mediante prácticas engañosas es considerado pretexto ilegal.

El sitio Web de la Comisión federal de comercio aclara y proporciona más información a esta entrevista:

- Es ilegal utilizar afirmaciones o documentos falsos, fraudulentos o ficticios para obtener información de clientes de una institución financiera o directamente del cliente de una institución financiera.
- Es ilegal utilizar documentos falsificados, perdidos o robados para obtener información de clientes de una institución financiera o directamente del cliente de una institución financiera.
- Es ilegal pedirle a una persona que consiga información de cliente de otra utilizando afirmaciones o documentos falsos, fraudulentos o ficticios o documentos falsificados, perdidos o robados.

Aunque la Comisión federal se centra en las instituciones financieras, las directrices establecidas son un recordatorio de lo que es ilegal en Estados Unidos. Es importante para un auditor estudiar las leyes locales y asegurarse de no violarlas. En 2006, la Comisión federal de comercio extendió la sección 5 de la ley de comercio para incluir una norma que prohibiera específicamente la utilización del pretexto para obtener registros telefónicos.

La situación de HP acabó con uno de los investigadores privados acusado de conspiración y robo de identidad federal, cargos muy graves.

Para mantenerse en la legalidad cuando ejecute sus pretextos deberá investigar un poco y definir claramente un plan aprobando los pretextos que se vayan a utilizar.

Independientemente de las consideraciones legales mencionadas, utilizar un pretexto sólido es una de las maneras más rápidas de acceder a una empresa. El pretexto es un talento en sí mismo y, como puede comprobar en este capítulo, no consiste simplemente en ponerse una peluca y unas gafas de sol y pretender ser quien no es.

Herramientas adicionales

Existen otras herramientas que pueden mejorar su pretexto.

Los elementos añadidos pueden ayudar mucho a convencer al objetivo de que su pretexto es real; por ejemplo, señales magnéticas en su coche, uniformes o disfraces, herramientas u otros elementos y, lo más importante, una tarjeta de visita.

Me di cuenta del poder de las tarjetas de visita en el aeropuerto recientemente, cuando me disponía a volar a Las Vegas en viaje de negocios. Siempre escanean la bolsa de mi portátil una y otra vez y la analizan en busca de restos de explosivos y ese tipo de cosas. Soy de los que no le importa soportar algunas medidas de seguridad de más, porque evitan que explote en el aire y eso me parece bien.

Pero me he dado cuenta de que el 90 por 100 de las veces capto la atención de los agentes de seguridad. En este viaje olvidé sacar de la bolsa del portátil mis ganzúas, el escáner de RFID, cuatro discos duros, llaves maestras (véase el capítulo 7) y una gran cantidad de artilugios de hacker. Mientras la bolsa pasaba por el escáner, escuché que la mujer que controlaba los rayos X decía: "Qué demonios...".

Llamó a otro agente que miró la pantalla y dijo: "No tengo ni idea de para qué diablos sirve todo eso". Después levantó la vista, se topó con mi cara sonriente y me dijo: "¿Esto es suyo?".

Fui hasta la mesa con él. Mientras sacaba de la bolsa mi escáner de RFID y mi caja de ganzúas dijo: "¿Por qué tiene todos estos artilugios y para qué sirven?".

No tenía nada planeado pero en el último momento se me ocurrió lo siguiente: saqué una tarjeta de visita y dije: "Soy un profesional de la seguridad especializado en probar redes, edificios y agujeros de seguridad. Éstas son mis herramientas de trabajo". Dije esto mientras le entregaba mi tarjeta. La miró unos cinco segundos y dijo: "Ah, perfecto. Gracias por la aclaración".

Guardó mis cosas cuidadosamente, cerró la bolsa y me dejó marchar. Normalmente, tengo que pasar por el detector de explosivos y un cacheo pero esta vez me dieron las gracias y me soltaron enseguida. Analicé qué había hecho

distinto a lo normal. La única diferencia era que le había dado una tarjeta de visita. Por supuesto, mis tarjetas no son de las baratas que se consiguen en Internet, pero me parecía increíble que la tarjeta hubiera dado un sentido de legitimidad a mis argumentos.

En mis siguientes cuatro vuelos puse todo el equipo profesional que pude en las bolsas y llevé mi tarjeta en el bolsillo. Cada vez que examinaban la bolsa y me preguntaban por su contenido, sacaba la tarjeta. En todas las ocasiones me pidieron disculpas, guardaron mis cosas y me dejaron marchar.

Imagine que esta experiencia hubiera sido un pretexto. Los pequeños detalles pueden otorgar tanto peso a mis argumentos que puedo resultar legítimo, verídico y sólido sólo con una tarjeta que convence a la gente de que todo lo que digo es cierto. No subestime el poder de una tarjeta de visita. Una advertencia: una tarjeta de mala calidad y aspecto miserable puede provocar el efecto contrario. Una tarjeta de visita gratuita con un anuncio en el reverso no añade peso a su pretexto profesional. Tampoco tiene sentido gastar 300 euros en unas tarjetas que se van a utilizar una sola vez. Muchas impresoras *on-line* pueden imprimir una pequeña cantidad de tarjetas con buen aspecto por menos de 100 euros.

Otro motivo para tomarse este capítulo muy en serio es que en muchas ocasiones el pretexto es el primer paso que dan los ladrones de identidad profesionales. Ya que el robo de identidad ha cobrado protagonismo en el panorama delictivo últimamente, saber lo que es y cómo identificarlo es importante para los consumidores, las empresas y los profesionales de la seguridad. Si es un auditor de seguridad debe ayudar a sus clientes a ser conscientes de estas amenazas y comprobar sus posibles debilidades.

Resumen

Además de explicar ampliamente el pretexto y proporcionar ejemplos reales de cómo funciona, este capítulo repasa los principios psicológicos que afectan a los distintos aspectos del pretexto. El siguiente paso lógico aborda justo eso: las habilidades mentales que los ingenieros sociales utilizan para parecer maestros del control mental y para tomar ventaja en su camino al éxito.

5. Trucos mentales: los principios psicológicos utilizados en ingeniería social

Todo depende de cómo vemos las cosas y no de cómo son en realidad.
Carl Gustav Jung

En el cine de Hollywood y en las series de televisión siempre se retrata a los estafadores y a los agentes de la ley con talentos casi místicos. Tienen la habilidad de resolver cualquier situación; simplemente mirando a los ojos a una persona, saben si está mintiendo o diciendo la verdad. Es habitual ver escenas como éstas: el policía mira a los ojos al sospechoso e inmediatamente sabe si miente o, simplemente con el poder de la sugestión, las víctimas de un estafador le entregan sus ahorros de toda la vida. Las películas pueden hacerle creer que las tácticas de manipulación son posibles e incluso fáciles de llevar a cabo. ¿Son ficticias estas situaciones? ¿Es posible desarrollar estas habilidades que se reservan para la fantasía de las películas?

Este capítulo podría ser un libro por sí solo pero sintetizaré esta información en principios que cambiarán el modo en que interactúa con la gente. Algunos de los temas desarrollados se basan en la investigación de las mentes más brillantes de sus respectivos campos. Las técnicas explicadas han sido probadas y evaluadas en entornos de ingeniería social. Por ejemplo, el tema de las microexpresiones se basa en la investigación del mundialmente famoso doctor Paul Ekman, que utilizó su

gran talento para desarrollar técnicas para leer las expresiones faciales, cambiando literalmente el modo en que las fuerzas del orden, los gobiernos, los médicos y la gente corriente interactúan con los demás.

Algunos de los principios establecidos por Richard Brandler y John Grinder, los creadores de la programación neurolingüística, revolucionaron la comprensión de los patrones de pensamiento y del poder de las palabras. Estos temas son el objeto de mucho debate y este capítulo pretende desmitificarlos y explicar cómo pueden utilizarse.

Algunos de los mejores interrogadores del planeta desarrollaron modos de entrenamiento y bases teóricas para ayudar a las fuerzas del orden a interrogar de manera efectiva a sus sospechosos. Estos principios tienen una raíz psicológica tan profunda que aprender los métodos empleados puede abrir literalmente las puertas de la mente de sus objetivos.

Utilizando las pistas que la gente da al hablar con sus gestos, sus ojos y sus caras, parecerá un auténtico lector de mentes. Este capítulo examina estas habilidades y las explica en detalle para que puedan utilizarse en el ámbito profesional.

"Compenetración" es una palabra usada frecuentemente por los formadores en el campo de las ventas y por los comerciales y es un aspecto muy importante para ganar y generar confianza. Aprender a desarrollar compenetración al instante con cualquier persona es una técnica que mejorará en gran medida sus habilidades como auditor de seguridad.

El capítulo termina con mis investigaciones personales sobre cómo piratear la mente humana. Un "desbordamiento de búfer" es un programa escrito normalmente por un hacker para ejecutar código malicioso dentro del proceso normal del host. Cuando se ejecuta, el programa hace lo que el hacker desee. ¿Qué pasaría si fuera posible activar "comandos" en la mente humana que provoquen que el objetivo haga lo que le pida, le dé la información que está buscando y, en resumen, prueben que la mente humana puede ser manipulada?

Por supuesto, esta información tan poderosa se puede utilizar con muy malas intenciones. Mi pretensión al revelar este conocimiento al público es descubrir lo que están haciendo los "chicos malos" poniendo en evidencia sus métodos, maneras de pensar y principios, para después analizarlos y mostrar lo que se puede aprender de ellos. Poner al descubierto estas técnicas hace más sencillo identificar, defenderse y reducir los efectos de estos ataques.

Este capítulo es una colección realmente impactante de datos y principios. Estudiar e investigar estos métodos no sólo mejorará sus actuaciones de seguridad, también cambiará la forma en que se comunica con los demás.

Bajo ningún concepto se explican aquí todos los aspectos de cada una de estas habilidades. Proporciono vínculos y consejos sobre dónde debe acudir para encontrar más información y sobre programas que ayudan a mejorar estas técnicas.

El capítulo crea una base y actúa como guía, señalándole el camino para mejorar cada técnica con el paso del tiempo.

El proceso para aprender estas habilidades es lento, así que debe ser paciente. Puede llevarle años perfeccionar algunos de esto métodos de aprendizaje y se requiere mucha práctica para dominarlos. Por supuesto, puede que ya posea alguna de estas habilidades pero, si no es así, tenga paciencia para aprenderlas. Trabaje duro practicándolas y lo conseguirá. Antes de meternos de lleno en el capítulo, la siguiente sección proporciona los fundamentos que explican por qué y cómo funcionan estos principios. Debe comprender las modalidades sensoriales o sistemas representacionales que existen. Cuando entienda claramente cómo recibe y procesa la información la gente, empezará a comprender las representaciones emocionales, psicológicas y físicas de ese proceso.

Las modalidades sensoriales

Para poder alterar la manera de pensar de alguien, debe comprender la "forma" y el "modo" en que esa persona piensa. Éste es el primer paso del proceso.

Puede que crea que hace falta ser psicólogo o neurólogo para comprender los aspectos relativos a cómo piensa una persona, pero no es así. Con investigación y aplicación práctica, puede profundizar en los procedimientos de la mente humana.

En agosto de 2001, el FBI sacó a la luz un comunicado de orden público (`www.social-engineer.org/wiki/archives/ModesOfThinking/MOT_FBI_3of5.htm`) que incluía algunas afirmaciones sobre las modalidades de pensamiento humano:

Simplemente confirmando su conducta no verbal ante el cliente, utilizando un lenguaje del sistema representacional preferencial del cliente e igualando su volumen, su tono de voz y su área de lenguaje, a menudo será suficiente para superar el rechazo del cliente a comunicarse.

Esta simple afirmación tiene un gran calado. Básicamente, significa que si puede descubrir cuál es la modalidad sensorial o sistema representacional preferencial del sujeto y después confirmar esa modalidad de manera sutil, puede desbloquear las puertas de su mente y ayudarle a sentirse cómodo contándole cualquier tipo de información. Lógicamente, se preguntará: "¿Cómo descubro la modalidad preferencial del sujeto?". Preguntarle a alguien cuál es su modalidad sensorial no es la forma más adecuada, porque la mayoría de la gente ni siquiera sabe lo que es. Por eso, debe contar con ciertas herramientas que le ayuden a determinar la modalidad de su objetivo para tomar medidas rápidamente para ajustarse a esa modalidad. Existe un camino claro y sencillo para conseguirlo, pero primero debe saber lo más básico.

Los sentidos

Los filósofos han discutido durante siglos el valor de la percepción. Algunos han llegado a afirmar que la realidad no es "real" sino sólo lo que nuestros sentidos perciben. Personalmente, no estoy de acuerdo con esta idea, pero sí creo que el mundo entra en nuestro cerebro a través de los sentidos. La gente interpreta esos sentidos como su percepción de la realidad. Según la clasificación tradicional, tenemos cinco sentidos: vista, oído, tacto, olfato y gusto.

La gente tiende a favorecer el uso de uno de esos sentidos y ése es el que se denomina preferencial. Ese sentido también determina la manera en que la gente tiende a recordar las cosas. Pruebe este ejercicio para determinar cuál es su sentido preferencial: cierre los ojos e imagínese a sí mismo levantándose esta mañana. ¿Qué es lo primero que recuerda?

¿Fue la "sensación" del sol en su cara? ¿O quizá recuerda el "sonido" de la voz de su pareja o sus hijos llamándole? ¿Recuerda claramente el olor del café en la cocina? ¿O quizá el mal "sabor" de boca, que le recuerda que tiene que limpiarse los dientes?

Por supuesto, esto no es una ciencia exacta y para determinar su sentido preferencial puede necesitar varios intentos. Una vez comenté estos conceptos con una pareja y sus respuestas fueron interesantes. Lo primero que recordaba la mujer al levantarse era mirar el reloj y preocuparse porque llegaba tarde, mientras que el primer recuerdo del marido era darse la vuelta en la cama y no sentir a su mujer a su lado. Después de unas cuantas preguntas más resultó evidente que el marido era cinestésico, es decir, su sentido preferencial era el tacto, mientras que su mujer era una persona muy visual.

Evidentemente, acercarse a su objetivo y decirle: "Cierra los ojos y dime tu primer recuerdo de esta mañana al levantarte", no parece muy razonable. Lo normal es que encuentre cierta oposición por este camino.

¿Cómo puede determinar, sin pasar por un interrogatorio embarazoso sobre sus rituales matutinos, cuál es el sentido preferencial de un sujeto?

Las tres modalidades sensoriales básicas

Aunque tenemos cinco sentidos, las modalidades sensoriales están asociadas con tres de ellos solamente:

- La vista o el pensador visual.
- El oído o el pensador auditivo.
- El tacto o el pensador cinestésico.

Cada sentido trabaja dentro de un registro o "submodalidad". ¿Algo está demasiado alto o demasiado bajo? ¿Es muy brillante o muy oscuro? ¿Está muy caliente o muy frío? Éstos son algunos ejemplos: el sol es muy brillante, el motor de un avión suena demasiado alto y 30 grados bajo cero es demasiado frío. Ivan Pavlov llevó a cabo un experimento en el que hacía sonar una campanilla cada vez que daba de comer a un perro. Al final, cuando el perro oía la campanilla empezaba a salivar. Lo que la mayoría de gente no sabe es que Pavlov estaba más interesado en los aspectos físicos y emocionales de las submodalidades. Lo interesante era comprobar que cuanto más alto sonaba la campana, más salivaba el perro. El cambio de registro de la submodalidad provocaba un cambio físico directo. La investigación de Pavlov y todas sus enseñanzas se explican en mucho más detalle en `www.ivanpavlov.com`.

Aunque las personas son muy diferentes de los perros, la investigación de Pavlov es muy importante para entender cómo piensa el ser humano. Muchos de nosotros podemos pensar en todas las modalidades pero tenemos una preferencial; una de ellas "suena" más fuerte. Y dentro de este sentido preferencial existen varios grados de profundidad.

A continuación, explicamos cada una de estas modalidades.

El pensador visual

La mayoría de la gente es pensadora "visual", en el sentido de que normalmente recuerdan el aspecto que tienen las cosas. Recuerdan claramente una escena: los colores, las texturas, la claridad u oscuridad. Pueden representar mentalmente la imagen de un evento pasado e incluso crear una imagen de un evento futuro. Cuando se les presenta algún asunto sobre el que tienen que decidir, normalmente necesitan ver algo porque esa aportación visual está directamente relacionada con la toma de decisiones. Muchas veces el pensador visual tomará una decisión en base a lo que le atrae visualmente sin importarle lo que en realidad es "mejor" para él.

Aunque los hombres tienden a ser visuales, esto no quiere decir que todos lo sean. Es verdad que el marketing visual o los aspectos visuales atraen a los hombres, pero no dé por hecho que todos los hombres son pensadores visuales.

Una persona visual utiliza a menudo ciertas expresiones, como:

- "Ya veo lo que quieres decir".
- "Eso tiene buena pinta".
- "Me lo imagino".

El registro en el que trabaja el sentido preferente en un pensador visual puede tener ciertas características o submodalidades, como:

- Luminosidad (brillante u oscuro).
- Tamaño (grande o pequeño).
- Color (blanco y negro o color).
- Movimiento (rápido o lento).
- Enfoque (claro o brumoso).

Es muy difícil, sino imposible, intentar debatir, negociar, manipular o influenciar a un pensador visual sin aportar elementos visuales. Los necesitan para tomar decisiones.

El pensador auditivo

Los pensadores auditivos recuerdan los sonidos de un evento. Recuerdan que la alarma sonaba demasiado alta o que una mujer susurraba demasiado bajo. Rememoran la dulzura de la voz de un niño o el intimidante ladrido de un perro.

La gente auditiva aprende mejor de lo que oye y puede retener mucha más información de lo que se les cuenta que de lo que se les enseña.

Debido a que un pensador auditivo recuerda el modo en el que suenan las cosas o debido a que los propios sonidos evocan recuerdos, utiliza frases como:

- "Alto y claro..."
- "Algo me dice que..."
- "Eso suena bien".

Y en el registro de este sentido preferente se encuentran todas estas submodalidades:

- Volumen (alto o bajo).
- Tono (bajo o agudo).
- Grado (alto o bajo).
- Ritmo (rápido o lento).
- Distancia (lejos o cerca).

Con los pensadores auditivos es fundamental elegir cuidadosamente las palabras. Las palabras que oigan serán claves. He visto cómo se echaban a perder estupendas ocasiones con pensadores auditivos por una única palabra equivocada.

El pensador cinestésico

Los "pensadores cinestésicos" se centran en las sensaciones. Recuerdan cómo les hizo sentir un evento: la calidez de una habitación, la suave brisa rozando su piel, el sobresalto en el cine con la película de terror. A menudo, a estas personas les gusta sentir los objetos tocándolos con las manos.

No es lo mismo decirles que una cosa es suave a dejarles que lo comprueben por sí mismos. Pero ayudarles a recordar un objeto suave que han tocado antes puede hacer que vengan a su mente emociones y sentimientos que son muy reales para ellos.

El término "cinestesia" está relacionado con lo táctil, lo visceral y la consciencia del propio cuerpo; básicamente, el reconocimiento del propio cuerpo en el espacio y de lo que las cosas le hacen sentir. Un pensador kinestésico utiliza frases como:

- "Capto la idea".
- "¿Qué te parece?".
- "Nos mantenemos en contacto".
- "Sólo quería darle un toque".
- "¿Qué se siente?".

El registro de este tipo de pensador puede tener las siguientes submodalidades:

- Intensidad (fuerte o débil).
- Área (grande o pequeña).
- Textura (áspera o suave).
- Temperatura (caliente o frío).
- Peso (pesado o ligero).

Al conseguir que un pensador cinestésico recuerde un sentimiento o emoción asociado a algo, puede hace que esos sentimientos reaparezcan tan reales como la primera vez. Para las personas no cinestésicas estos pensadores son los más difíciles de manejar porque no reaccionan a imágenes o sonidos y hay que contactar con sus sentimientos para comunicarse con ellos.

Entender estos principios básicos le ayudará a decidir rápidamente qué tipo de persona es su interlocutor. De nuevo, sin poder preguntar al objetivo su primer recuerdo del día, ¿cómo puede distinguir el sentido preferente? Es más, ¿por qué es tan importante?

Determinar el sentido preferente

La clave para determinar el sentido preferente es presentarse a alguien, empezar una conversación y permanecer muy atento a lo que dice. Cuando se acerca al objetivo para saludarlo, puede que prácticamente no le mire. En ese caso, a lo mejor es un poco grosero o puede que no sea un pensador visual. Las personas visuales necesitan mirar a la persona con la que hablan para comunicarse adecuadamente, por lo que este comportamiento puede significar que no es visual. Después, pregunte algo sencillo como: "¿No le agrada la sensación de un bonito día como hoy?" y fíjese en su respuesta y, sobre todo, en su reacción.

Puede que usted lleve puesto un gran anillo de plata brillante. Gesticule al hablar; quizá el anillo llame su atención. ¿Estira el brazo para intentar tocarlo o se acerca para observarlo? Las personas cinestésicas necesitan tocar las cosas. Conozco a una mujer muy cinestésica que cuando ve algo que considera que es suave o de buena calidad "necesita" tocarlo. Dice cosas como: "¡Vaya! Ese jersey parece muy suave". Por esa afirmación se podría creer que es visual, pero lo que sucede a continuación despeja la duda. Se acerca a la persona y toca el jersey. Esto muestra que su sentido preferente es el cinestésico. Esa misma mujer tiene que tocar todos los productos que ve cuando va de compras. Tocando los objetos crea una conexión que los hace reales para ella. Normalmente, no recuerda muy bien las cosas con las que no ha tenido contacto físico.

Hacer preguntas que contengan las palabras clave, observar las reacciones del objetivo y "escuchar" pueden revelar su sentido preferente. Prestar atención a las palabras clave como "ver", "escuchar", "brillante", "oscuro" puede llevarle a determinar que un objetivo es visual, por ejemplo. Como ya hemos dicho, esto no es una ciencia exacta. No existe una norma general que establezca que si una persona dice "ya veo lo que quieres decir" signifique que con toda seguridad esa persona sea visual. Cada pista debe acercarle a la confirmación de su corazonada haciendo más preguntas y averiguaciones.

Una advertencia: hablarle a alguien en un sistema representacional distinto del que emplea normalmente, puede molestar a algunas personas. Por otra parte, utilizar preguntas para determinar el sistema representacional de una persona puede resultar incómodo. Haga las preguntas con moderación y apóyese más en la observación.

Por qué es tan importante entender la modalidad

En cierta ocasión, trabajé con un tipo, Tony, que podía venderle un vaso de agua a un hombre que se estuviera ahogando. A Tony le gustaba mucho emplear la técnica de descubrir y después utilizar el sentido preferente de las personas. Utilizaba

varios métodos para ello. En el primer contacto con el objetivo, siempre sostenía en la mano un bolígrafo muy brillante de oro y plata. Gesticulaba mucho con él y se fijaba en el objetivo para ver si estaba siguiendo el bolígrafo con la mirada; si notaba que lo seguía ligeramente, exageraba los gestos para comprobar qué hacía con los ojos. Si no obtenía resultados en los primeros segundos, empezaba a pulsar repetidamente el botón del bolígrafo. No era un sonido muy alto, pero sí lo suficiente como para distraer una línea de pensamiento y llamar la atención de una persona auditiva. Si creía que esto estaba funcionando, pulsaba el botón del bolígrafo con cada pensamiento o afirmación importante, haciendo que el objetivo tuviera una reacción psicológica al sonido y a lo que se estaba diciendo. Si esta táctica tampoco daba resultado, estiraba el brazo por encima de la mesa y daba golpecitos en la muñeca o el antebrazo del objetivo o, si estaba lo suficientemente cerca, le tocaba el hombro. Observaba sus reacciones para comprobar si se apartaba o si parecía alegrarse o molestarse por el contacto.

Con estos métodos sutiles podía descubrir rápidamente cuál era el sentido preferente de una persona. Todo el proceso no le llevaba más de un minuto. Una vez que obtenía la información que buscaba, empezaba a dirigir la conversación hacia ese sentido preferente, incluso adoptando los rasgos característicos de ese sentido en la forma en que hablaba y en el modo de actuar y de reaccionar en la conversación. Tony cerró más ventas que cualquier otra persona que conozca. A menudo la gente decía sobre él: "Es como si supiera exactamente lo que necesito".

Tony hablaba a las personas de la forma en que les gustaba que les hablaran. Si la persona era pensadora visual, Tony decía cosas como: "¿Ves lo que quiero decir?" o "¿Cómo lo ves?". Utilizaba ilustraciones que implicaran "ver" las cosas o visualizar escenarios. Ponía a la gente en su elemento.

La gente está cómoda cuando está en su elemento. Cuanto más pueda hacer por que la gente se encuentre cómoda, mayores probabilidades de éxito tendrá. La gente gravita hacia las personas con las que se siente bien; es la naturaleza humana. Por ejemplo, si alguien le hace sentir "cómodo y a gusto" o parece entender lo que dice y sus motivaciones y argumentos, se abrirá a esa persona con facilidad confiando en ella e integrándola en su círculo.

Quiero reiterar este punto: encontrar y utilizar el sentido preferente de una persona no es una ciencia exacta. Debe utilizarse como una herramienta más del arsenal y no depender de ello como si fuera algo científico o mágico. Algunos aspectos psicológicos de la naturaleza humana sí se basan en ciencia demostrada y se puede contar con ellos. De hecho, algunos de estos aspectos son tan asombrosos que pueden hacer que parezca un lector de la mente. Han sido el tema de mucho debate y algunos han sido aceptados por psicólogos, fuerzas del orden e ingenieros sociales desde hace años. Las siguientes secciones del capítulo explican estos conceptos, empezando por las microexpresiones.

Las microexpresiones

Seguramente, está familiarizado con la idea de leer las expresiones faciales. Cuando alguien está contento, triste o enfadado, cuando alguien tiene algún sentimiento, se puede observar su rostro y ver ese sentimiento. ¿Qué pasaría si alguien intentara imitar esa expresión, como con una sonrisa falsa? A todos nos ha pasado, vamos caminando por el supermercado y nos encontramos con alguien que conocemos pero que no nos gusta mucho. Ponemos una "sonrisa" y decimos: "Hola, John, me alegro de verte. Saluda a Sally de mi parte".

Podemos actuar con cortesía pero en el fondo nos sentimos molestos. Las expresiones que mostramos en nuestro rostro durante periodos de tiempo largos se llaman macroexpresiones y con ellas es fácil ver el sentimiento que se está transmitiendo. Al igual que las microexpresiones, las macroexpresiones se controlan con nuestros sentimientos, pero no son involuntarias y normalmente se pueden fingir.

Unos cuantos pioneros en el estudio de la conducta humana han pasado décadas investigando lo que han denominado "microexpresiones", para entender cómo transmiten las emociones los humanos.

Las microexpresiones no pueden controlarse fácilmente y ocurren como reacción a los sentimientos. Un sentimiento dispara ciertas reacciones musculares en el rostro que provocan que aparezca una expresión concreta. A menudo, esas expresiones duran tan solo una vigésimo quinta parte de segundo. Es prácticamente imposible controlarlas porque son movimientos musculares involuntarios de respuesta a un sentimiento o emoción.

Esta definición tampoco es nueva; Charles Darwin escribió en 1872 *La expresión de las emociones en los animales y en el hombre*. En él, Darwin señala la naturaleza universal de las expresiones faciales y cómo se utilizan los músculos en ellas.

A principio de los años sesenta dos investigadores, Haggard e Isaacs, descubrieron lo que hoy llamamos microexpresiones. En 1966, Haggard e Isaacs explicaron cómo descubrieron estas expresiones "micromomentáneas" en una publicación titulada *Micromomentary Facial Expressions as Indicators of Ego Mechanisms in Psychotherapy* (Las expresiones faciales micromomentáneas como indicadores de los mecanismos del ego en psicoterapia).

También en 1960, William Condon, un pionero que estudió horas de cintas, fotograma a fotograma, descubrió que los humanos realizaban "micro-movimientos". También investigó mucho en materia de programación neurolingüística (trataremos más adelante este tema) y lenguaje corporal.

Probablemente, uno de los investigadores más influyentes en el campo de las microexpresiones es el doctor Paul Ekman, que convirtió las microexpresiones en la ciencia que es hoy en día. El doctor Ekman ha estado estudiando las microex-

presiones durante más de cuarenta años, ha sido galardonado con el Research Scientist Award (Premio de investigación científica) y fue nombrado como una de las personas más influyentes del 2009 por la revista *Time*.

El doctor Ekman investigó las expresiones faciales con el psicólogo Silvan Tomkins. Su investigación reveló que, contrariamente a la creencia popular, las emociones no están determinadas culturalmente sino que son biológicas y universales a través de todas las culturas.

Trabajando junto a la doctora Maureen O'Sullivan, desarrolló un proyecto llamado *Wizards Project* (El proyecto del genio). Fue el primero en utilizar las microexpresiones para la detección de mentiras. Utilizó una base de 15.000 personas de todas las culturas y clases sociales y descubrió que sólo 50 de todas esas personas tenían la habilidad de descubrir un engaño sin entrenamiento previo.

En los años setenta el doctor Ekman desarrolló el "sistema de codificación facial de acciones" (FACS, *Facial Action Coding System*) para etiquetar y numerar todas las expresiones humanas concebibles. Su trabajo evolucionó para integrar, no sólo las expresiones faciales, sino también cómo se involucra el cuerpo completo en realizar el engaño. En el año 1972, el doctor Ekman había identificado una lista de expresiones que se relacionaban con emociones básicas o biológicamente universales:

- Ira.
- Repugnancia.
- Miedo.
- Alegría.
- Tristeza.
- Sorpresa.

El trabajo del doctor Ekman empezó a seguirse desde entornos empresariales y gubernamentales, que comenzaron a utilizar su investigación para detectar el engaño. En 1990, en una ponencia titulada "Basic Emotions" (Emociones elementales), el doctor revisó su lista original para incluir una serie de emociones positivas y negativas (`www.paulekman.com/wp-content/uploads/2009/02/Basic-Emotions.pdf`). El doctor Ekman ha publicado muchos libros sobre emociones, expresiones faciales y detección de mentiras que pueden ayudar a comprender el valor de ser capaz de descifrar las expresiones faciales.

Esta historia demuestra que la idea de las microexpresiones no es una fantasía sino todo lo contrario; médicos, investigadores y profesionales del campo de la conducta humana han dedicado incontables horas a estudiarlas y comprenderlas. Como ingeniero social, comprender las microexpresiones le será de gran ayuda a la hora de proteger a sus clientes y enseñarles cómo detectar pequeñas señales de engaño.

Recomiendo la lectura de todos los libros del doctor Ekman, especialmente *Emotions Revealed* (Emociones al descubierto) y *Unmasking the Face* (Desenmascarar el rostro). Es una auténtica autoridad en este terreno. Las siguientes secciones explican brevemente las microexpresiones para que pueda empezar a utilizarlas en su trabajo como profesional de la seguridad.

Como ya hemos comentado, el doctor Ekman catalogó seis microexpresiones principales y después añadió el desprecio a la lista, para formar un total de siete. A continuación, las explicamos una a una.

Ira

La ira o el enfado se detecta normalmente con más facilidad que otras expresiones. Los labios se estrechan y se tensan. Las cejas se inclinan hacia abajo y se juntan. Y, por supuesto, está el rasgo más característico de la ira: la mirada.

La ira es una emoción muy fuerte que puede dar pie a otras muchas emociones. A veces, cuando alguien se enfada, puede ver una microexpresión como la que muestra la figura 5.1. Lo que lo hace difícil de detectar es que los movimientos faciales pueden durar sólo una vigésima quinta parte de segundo.

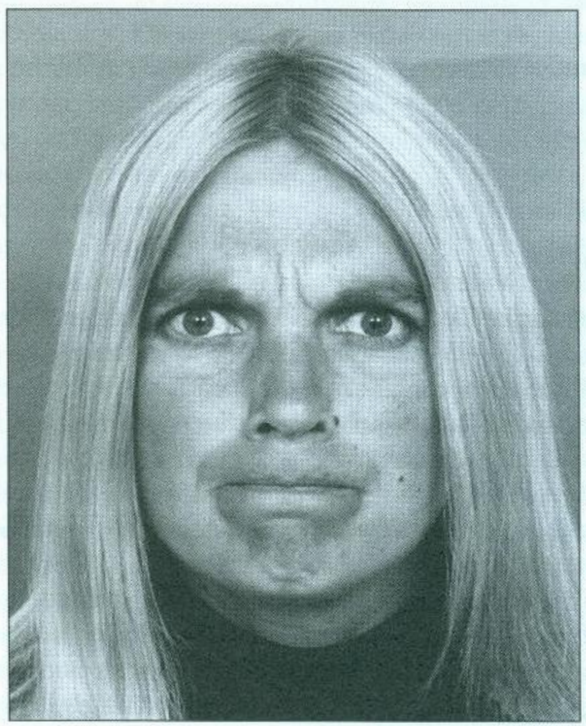


Figura 5.1. *Observe la mirada, los labios apretados y las cejas tensas.*

Aprender a detectar una microexpresión específica puede mejorar en gran medida su comprensión de las personas. Para lograrlo, el doctor Ekman recomienda que practique esa expresión siguiendo estos pasos:

1. Baje y junte las cejas, como si intentara tocar la nariz con la parte interna de las cejas.
2. Manteniendo las cejas bajas, intente abrir mucho los ojos (sin variar la posición de las cejas).
3. Apriete fuerte los labios. No los arrugue, sólo ténselos y júntelos.
4. Ponga una mirada feroz.

¿Qué siente al poner esta expresión? La primera vez que lo hice me invadió un fuerte sentimiento de ira. La siguiente afirmación es un punto fundamental de este capítulo:

Si mantener la expresión nos provoca una emoción, eso debe significar que nuestros movimientos faciales pueden afectar a nuestros sentimientos y puede que incluso a los sentimientos de quienes nos rodean.

Practique esta emoción delante de un espejo hasta que la ejecute correctamente. La figura 5.2 muestra la imagen de una mujer enseñándonos exactamente cómo se exterioriza la ira.

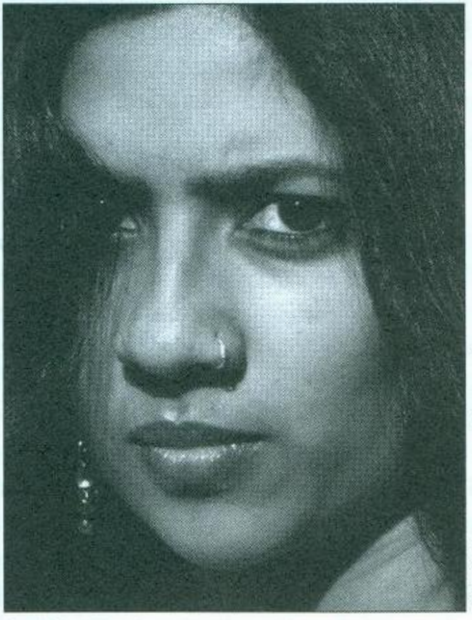


Figura 5.2. *Observe la expresión de ira evidente en el rostro.*

Es tan pronunciado como en la figura 5.1 y, además, la fría mirada revela también este sentimiento.

Dominar la habilidad de reproducir las microexpresiones le ayudará a comprender las emociones asociadas a ellas. Cuando pueda reproducir y descodificar una microexpresión podrá determinar la emoción que la está causando. En ese momento entenderá el estado mental en el que se encuentra su interlocutor. No sólo debe aprender a reproducirlas, también debe ser capaz de detectarlas en los demás. De esta forma, tendrá más control sobre el proceso de sus actuaciones profesionales.

Repugnancia

La repugnancia es una emoción intensa como reacción ante algo que le disgusta mucho. Este "algo" no tiene por qué ser un objeto físico; también puede basarse en una creencia o en un sentimiento.

Una comida que odia puede provocarle repugnancia haciendo aparecer esta expresión. Lo que resulta más interesante es que, aunque esa comida no esté a la vista ni pueda olerla, su simple recuerdo puede causar la misma emoción.

Cuando era joven fui a Disney World con unos amigos. A mí no me gustan nada, y quiero decir "nada", las montañas rusas. Después de que mis amigos insistieran mucho, subí a la *Space Mountain*, una montaña rusa que está instalada en un recinto cerrado. Llevábamos la mitad del recorrido y ya había decidido que no me disgustaban tanto las montañas rusas, cuando de pronto me pringó algo húmedo y espeso. Enseguida me llegó un olor que sólo puedo describir como de contenidos estomacales. No sólo yo, muchos detrás de mí tuvieron la misma reacción y no pudimos contener nuestro almuerzo, por decirlo de alguna manera. En un momento, un vómito colectivo salpicó los cristales de la *Tomorrowland Transit Autority*, un tren que hace un lento recorrido visitando Disney World y que pasa por el recinto de la *Space Mountain*. Lo más asombroso es que las personas que viajaban en el tren *Tomorrowland* vieron el vómito chocar contra el cristal mientras pasaban y nos vieron a nosotros con tan mal aspecto que ellos también vomitaron. Sin embargo, ellos no percibieron el olor ni tuvieron contacto físico con el vómito. Entonces, ¿por qué reaccionaron así?

Por repugnancia. Normalmente, los fluidos corporales provocan un sentimiento de repugnancia y ésa es la razón por la que mientras leía este párrafo seguramente haya manifestado expresiones de repugnancia.

Esta emoción se caracteriza por el labio superior levantado enseñando los dientes y la nariz arrugada. También pueden elevarse las mejillas al arrugar la nariz, como intentando bloquear el paso del mal olor o el pensamiento a la mente.

Lo que sea que acaba de ver el hombre de la figura 5.3 ha provocado una clara expresión de disgusto.

Mightyjohn. dreamstime.com

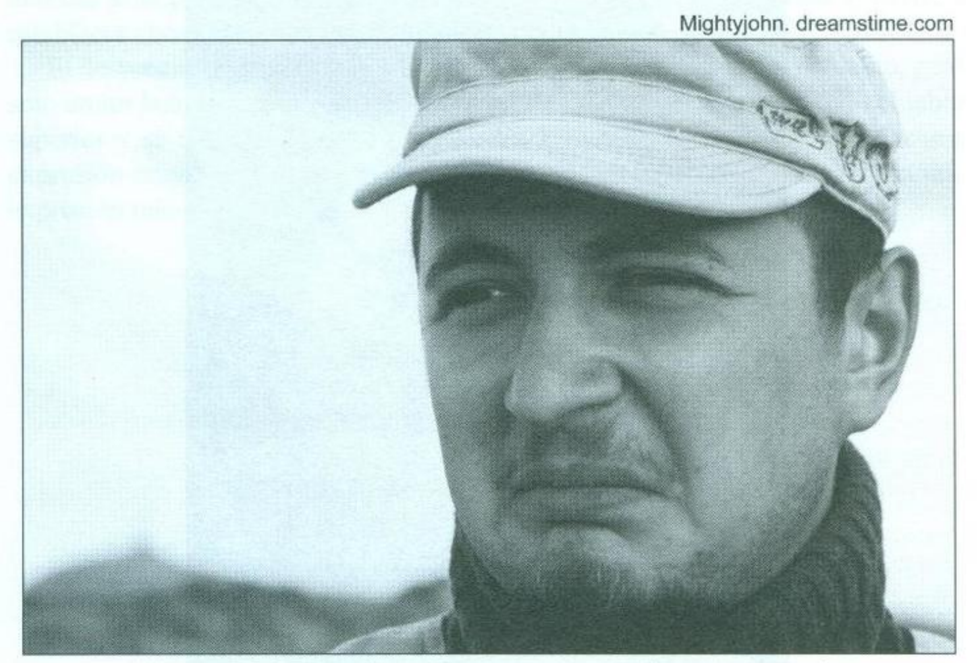


Figura 5.3. *Signos claros de repugnancia con la nariz arrugada y el labio superior levantado.*

Según la investigación del doctor Ekman, la repugnancia es una de las emociones que surge como reacción a la visión, olor o incluso recuerdo de algo desagradable. Desde el punto de vista de la ingeniería social, esta emoción no es un buen camino hacia el éxito pero le puede ayudar a comprobar si está dando en el clavo con su objetivo o si, por el contrario, está provocando que se cierre mentalmente a sus ideas.

Si por algún motivo provoca repugnancia en su objetivo, lo más probable es que esté perdido. Si su aspecto, estilo, olor, aliento u otro aspecto de su persona provoca que una persona sienta repugnancia, seguramente se le cerrarán las puertas del éxito.

Debe ser consciente de lo que sus objetivos toleran y lo que no. Por ejemplo, si va a realizar una auditoría para un prestigioso despacho de abogados y tiene muchos tatuajes y *piercings*, puede provocar un sentimiento muy negativo en su objetivo, que le rechazará. Si detecta una expresión facial parecida a la de la figura 5.4, ya sabe que es el momento de marcharse.

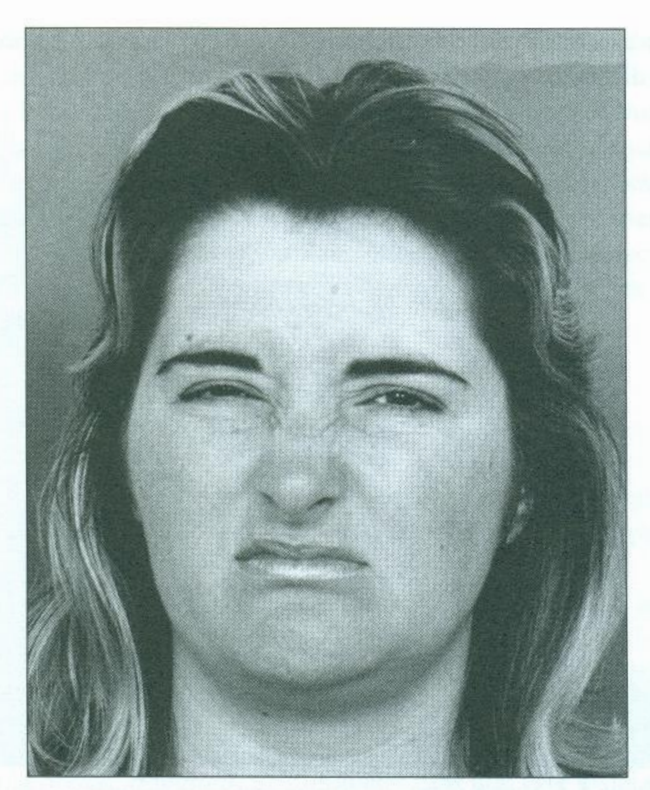


Figura 5.4. *Si detecta esta expresión, algo va mal.*

Debe tener muy en cuenta su aspecto cuando prepare su pretexto. Si detecta en su objetivo una emoción tan negativa como la repugnancia, debe considerar marcharse disculpándose educadamente y volver a preparar su pretexto o encontrar una nueva vía de acceso.

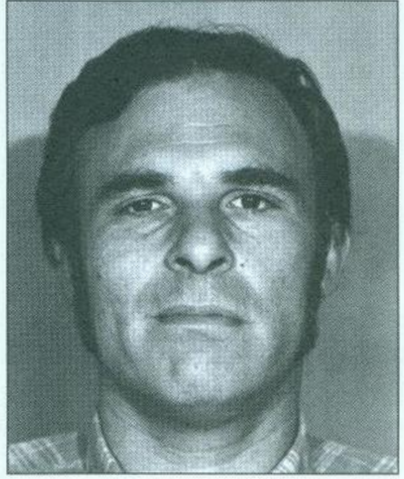
Desprecio

El desprecio es una emoción fuerte que se confunde a menudo con la repugnancia porque están muy relacionadas. El doctor Ekman ni siquiera incluyó el desprecio en su lista inicial de emociones fundamentales.

En su libro *Emotions Revealed* (Emociones al descubierto), el doctor Ekman dice: "El desprecio sólo se siente por personas o por actos de personas, pero no por sabores, olores o texturas". Pone el ejemplo de comer sesos, que puede resultar desagradable y provocar repugnancia. Sin embargo, ver a una persona comiéndolos puede provocar desprecio por la persona que los come, no por el acto en sí.

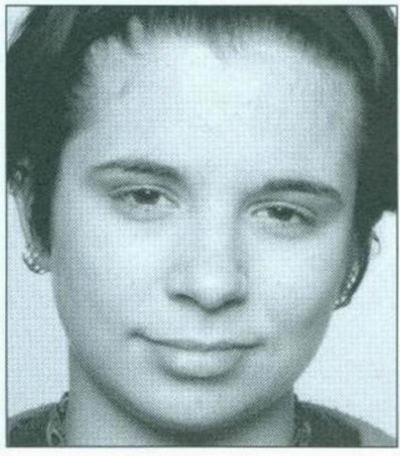
El hecho de que el desprecio va dirigido a una persona en lugar de a un objeto, es fundamental para comprender las microexpresiones que implica. Ser capaz de detectar si la persona con la que trata está sintiendo desprecio puede ayudarle a establecer con exactitud las causas de sus sentimientos.

El desprecio se caracteriza por la nariz arrugada y la elevación del labio, pero sólo en un lado de la cara, mientras que en la repugnancia se eleva todo el labio superior y se arruga la nariz completa. En la figura 5.5 se puede apreciar una expresión muy ligera de desprecio, mientras que en la figura 5.6 se muestra una expresión más evidente



Dr. Paul Ekman

Figura 5.5. *Observe la nariz ligeramente arrugada y la elevación del lado derecho del rostro del doctor Ekman.*



Dr. Paul Ekman

Figura 5.6. *Observe que los signos de desprecio son más pronunciados en esta imagen.*

Intente imitar desprecio y, si es como yo, enseguida sentirá ira y desprecio. Es interesante realizar este ejercicio y observar cómo le afectan emocionalmente las reacciones.

El desprecio muchas veces va acompañado de ira, porque los motivos que causan desprecio también pueden disparar otras emociones muy negativas. Ésta es una emoción que debe evitar que surja en la persona con la que está interactuando, sobre todo si lo hace en un ámbito profesional.

Miedo

El miedo se confunde a menudo con la sorpresa porque ambas emociones causan reacciones musculares parecidas en el rostro. Recientemente, volaba en un avión y me disponía a escribir la sección correspondiente a la alegría, cuando sucedió algo asombroso que me empujó a cambiar de idea y escribir la sección sobre el miedo.

Mido 1,92 metros y además soy corpulento. Estaba sentado en el avión con varias horas de vuelo por delante y pensé que podía aprovechar para trabajar. Permítame añadir que los asientos de los aviones ya no son lo que eran. Estaba sentado con mi portátil abierto, mirando al vacío y pensando cómo empezar la sección que pretendía escribir. Enseguida me di cuenta de que tenía que escribir sobre el miedo.

El caballero sentado a mi lado sacó una botella de agua, tomó un trago y después me pareció que no le ponía el tapón otra vez. Por el rabillo del ojo vi cómo se le caía la botella de las manos en dirección a mi portátil. Mi reacción inmediata podía interpretarse fácilmente como miedo.

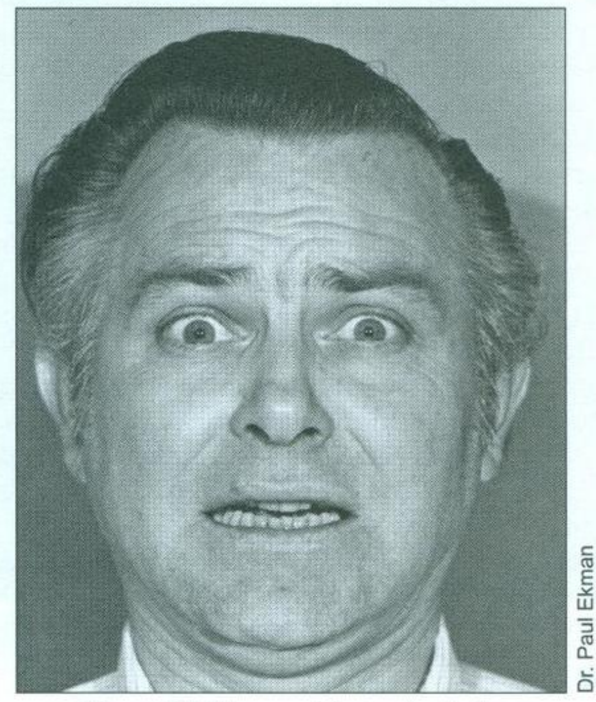
Abrí mucho los ojos, mientras mis cejas se juntaban hacia dentro. Mis labios se juntaron y tiraron hacia las orejas. Por supuesto, no me di cuenta de todo esto mientras sucedía, pero después pude analizar lo que había sucedido y supe que había sentido miedo. Analicé la forma en que se había movido mi rostro y pensé que si intentaba repetir esa expresión sentiría otra vez la misma emoción. Estoy seguro de que mi aspecto fue parecido al de la figura 5.7.

Intente provocar esta emoción siguiendo estos pasos:

1. Levante las cejas todo lo que pueda.
2. Deje caer la boca ligeramente abierta y tire de los extremos hacia atrás.
3. Si puede, junte las cejas mientras las eleva al máximo.

¿Cómo se siente? ¿Qué sensaciones tiene en las manos, los brazos y el estómago? ¿Nota algo parecido al miedo? Si no es así, intente este ejercicio otra vez pero piense en una situación del pasado que escapaba a su control (algo parecido

a mi experiencia en el avión o un coche frenando de golpe delante de usted). Compruebe cómo se siente entonces. Probablemente, sentirá esta emoción. Un amigo me envió esta fotografía de su hija montando en la montaña rusa por primera vez (figura 5.8). Puede ver claramente las cejas levantadas, ojos y boca muy abiertos y los labios estirados hacia atrás.



Dr. Paul Ekman

Figura 5.7. *Signos evidentes de miedo.*



Chad Skidmor

Figura 5.8. *Signos claros de miedo.*

Desde un punto de vista profesional, el miedo se utiliza para lograr que la gente reaccione de cierta manera. Los ingenieros sociales malintencionados utilizan tácticas de miedo para conseguir que un usuario desprevenido haga clic en un *banner* o revele una información valiosa. Por ejemplo, un *banner* malicioso puede anunciar: "Su ordenador está infectado con un virus. Haga clic aquí para arreglarlo ¡ahora!". Este tipo de *banner* se aprovecha de usuarios con pocos conocimientos técnicos que hacen clic y justo entonces su ordenador se infecta realmente.

Una empresa para la que trabajaba fue atacada por un individuo que utilizó el miedo para acceder al edificio. Entró en las oficinas haciendo el papel del técnico del servicio de asistencia. Sabía que el director general estaba fuera de la ciudad en una importante reunión de negocios y que no se le podía molestar, por lo que dijo: "El señor Smith, su director general, me llamó y me dijo que aprovechara ahora que está fuera en la reunión para arreglar su problema con el correo electrónico. Dijo que si no lo dejaba resuelto iban a rodar cabezas".

La secretaria temió que si no se solucionaba el problema podían culparla a ella también. ¿Podría enfadarse mucho su jefe? ¿Podía incluso poner en riesgo su trabajo? Al tener miedo de una reacción negativa de su jefe, dejó pasar al falso técnico. Si era un profesional bien preparado, se habría estado fijando en las expresiones faciales de la secretaria para detectar si mostraba preocupación o ansiedad, que están relacionados con el miedo. Después, podía haber insistido sobre estos signos para hundirla cada vez más en el miedo.

El miedo puede motivar mucho a una persona para hacer cosas que de otra forma no haría.

Sorpresa

Como hemos mencionado previamente, el doctor Ekman y muchos otros psicólogos del campo de las microexpresiones determinaron que la sorpresa está íntimamente relacionada con el miedo debido a ciertas similitudes. Aun así, existen algunas diferencias, como la dirección de los labios y el modo en que reaccionan los ojos.

Intente este ejercicio para mostrar sorpresa:

1. Eleve las cejas, no como en el caso del miedo, sino con el objetivo de abrir los ojos tanto como pueda.
2. Deje que se descuelgue la mandíbula y abra ligeramente la boca.
3. Cuando haya memorizado el movimiento, intente hacerlo deprisa.

Cuando hice este ejercicio noté que casi necesité dar una bocanada de aire, haciéndome sentir algo parecido a la sorpresa. Debe conseguir una expresión parecida a la de la figura 5.9.

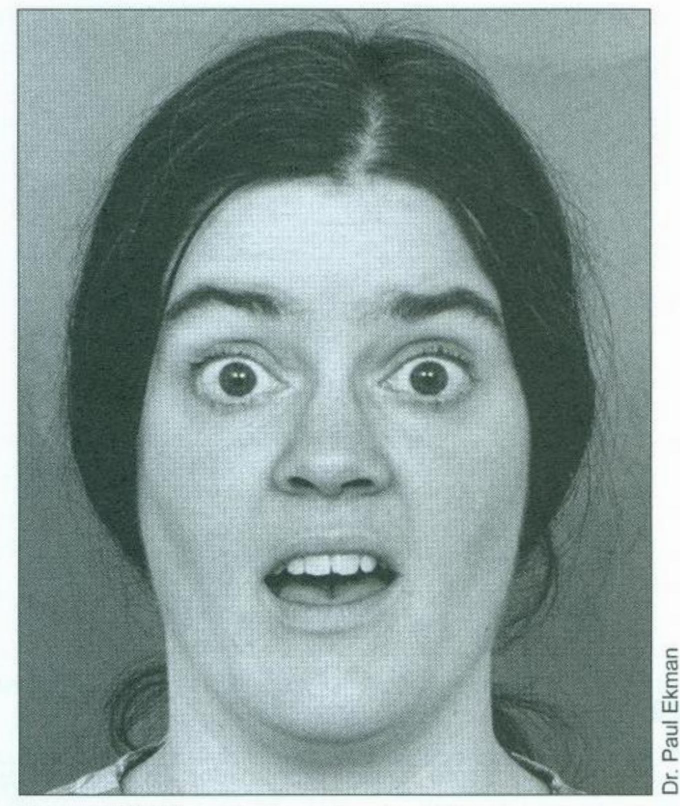


Figura 5.9. *Observe cómo el gesto de los ojos y las cejas es muy parecido al del miedo.*

La sorpresa puede ser buena o mala. Oír las primeras palabras de su hija, por supuesto, es una buena sorpresa.

También puede provocarla un evento, afirmación o pregunta que no se espera.

Como puede ver en la figura 5.10, lo que sea que haya visto esa mujer la ha sorprendido realmente. Quizá sea por un regalo que le han hecho o por algo que le ha dicho su nieto. Observe sus cejas levantadas y su mandíbula descolgada y abierta. Este tipo de sorpresa es fácil de ver porque es tan pronunciada que la expresión se detecta enseguida.

Si la sorpresa es positiva, a menudo provoca una sonrisa o una respuesta jovial después de que se desvanece el impacto inicial. Un ingeniero social puede utilizar la sorpresa para abrir al objetivo, por así decirlo; si después continúa con una ocurrencia o un chiste el objetivo se sentirá cómodo rápidamente y bajará la guardia.



Stylephotographs (Robert Kneschke). Dreamstime.com

Figura 5.10. *A veces la sorpresa se confunde con el miedo, pero hay pequeñas diferencias.*

Tristeza

La tristeza es un sentimiento fuerte y abrumador. Es uno de esas emociones que podemos sentir cuando vemos a otras personas experimentándola. Algunas personas se sienten tristes, llegando incluso a las lágrimas, simplemente por ver a otras personas tristes.

Para mostrarle lo sencillo que es sentir tristeza, intente lo siguiente:

1. Deje caer la boca ligeramente abierta.
2. Tire de los extremos de la boca hacia abajo.
3. Mantenga los labios en posición y mientras tanto intente levantar las mejillas como si quisiera entrecerrar los ojos.
4. Manteniendo esta posición, mire hacia abajo y deje que los parpados caigan.

Probablemente, empezará a sentirse triste. La primera vez que practiqué este ejercicio, la sensación fue abrumadora. Me sentí triste al instante y comprobé que tenía que tener cuidado con el tiempo que mantenía la expresión porque provocaba que me sintiera triste durante mucho tiempo. Compruebe el aspecto de esta expresión en la figura 5.11.

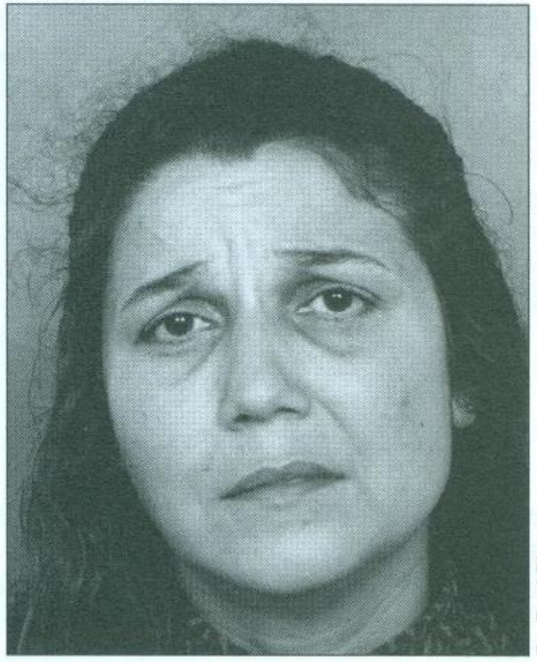


Figura 5.11. *Observe los labios y los ojos caídos, signos de tristeza.*

Otro aspecto de la tristeza que hace de ella una emoción increíble es que no siempre se manifiesta como desesperación o pena profunda. La tristeza puede ser muy sutil. También puede aparecer en un solo lado de la cara. La gente a veces intenta disimular la pena utilizando una sonrisa falsa o lo que yo llamo "ojos estoicos", con la mirada fija al frente, un poco aturdida, pero cuya expresión delata que está intentando controlar la emoción que siente. Observe la figura 5.12. En este caso puede ver un ejemplo de tristeza con la mitad del rostro cubierto. Esta mujer muestra claros signos de tristeza que pueden apreciarse a pesar de tener cubierta la mitad del rostro. Observe su frente ligeramente arrugada y sus cejas caídas. También puede ver las esquinas de su boca apuntando hacia abajo.

Los ojos son los mejores indicadores para detectar la tristeza. La expresión se confunde a menudo con el cansancio y otros sentimientos que pueden causar movimientos de ojos parecidos. Relacionar el lenguaje corporal con lo que se ve en el rostro puede ayudar a determinar si se trata de tristeza o de otra emoción.

Esto es especialmente válido cuando se trata de culturas diferentes a la suya. Especialmente en culturas donde se cubre gran parte del rostro. En muchos países del Oriente Medio, donde las mujeres se cubren el rostro, puede que sólo pueda ver los ojos de la persona. En estos casos es muy importante valerse del lenguaje corporal para determinar si lo que ve es realmente tristeza



Figura 5.12. Observe que los signos de tristeza son evidentes en sus ojos, cejas y labios.

La tristeza se utiliza mucho en ingeniería social porque puede provocar que la gente realice alguna acción como hacer un donativo o dar información. Probablemente, habrá visto cómo se utiliza en anuncios de televisión en los que muestran a niños desfavorecidos. Esos niños están malnutridos, hambrientos y faltos de cariño, pero con una pequeña donación puede poner una sonrisa en su rostro. La imagen de niños tristes, llorosos y escuálidos le llegará al corazón. No estoy diciendo que estos anuncios sean malintencionados, pero emplean en cierto modo la ingeniería social utilizando un activador emocional para lograr una reacción de su objetivo.

Desgraciadamente, los ingenieros sociales malintencionados utilizan a menudo este activador emocional para sonsacar a sus víctimas. En cierta ocasión, entré en un restaurante y escuché a un hombre diciendo a un grupo de personas mayores que estaba saliendo que se había quedado sin gasolina en la autopista y tenía que llegar a casa cuanto antes porque su mujer estaba embarazada de nueve meses. Había venido andando un kilómetro desde la autopista para llamar a su mujer y quería saber si le podían dejar 20 euros. Cuando empecé a escuchar la historia me acerqué haciendo creer que estaba llamando por teléfono y observé lo que sucedía después. Terminó de contar su historia y finalmente, para respaldarla, dijo: "Miren, si me dan su dirección les mando un cheque de 20 euros" y terminó con un "lo juro por Dios".

La historia tenía algunos elementos que provocaban compasión, sobre todo cuando su rostro mostraba preocupación, ansiedad y tristeza. No le dieron 20 euros, consiguió que cada una de las tres personas del grupo le diera un billete de 20. Dijo: "Que Dios os bendiga" varias veces, les abrazó y les dijo que iba a llamar a su mujer para decirle que estaba de camino a casa. Volvió a abrazarles y les dejó con la sensación de que habían hecho la buena obra de la semana.

Unos minutos después, vi a aquel tipo en la barra del restaurante tomando unas cuantas bebidas gratis con sus amigos. Mezclando una historia triste con unas cuantas expresiones faciales de tristeza, había conseguido manipular las emociones de la gente.

Felicidad

La felicidad tiene muchas facetas, tantas, que se podía escribir un capítulo entero sobre ella. El doctor Ekman explica varios puntos interesantes sobre la felicidad y otras emociones parecidas y cómo afecta a la persona experimentando esa emoción y a las personas a su alrededor.

Yo me quiero centrar en un par de aspectos de la felicidad, sobre todo en la diferencia entre una sonrisa verdadera y una falsa. Éste es un aspecto de las expresiones humanas que es importante saber detectar y saber reproducir.

¿Alguna vez ha conocido a alguien que parecía muy agradable pero después de separarse de él ha pensado: "Qué tipo más falso"?

Puede que no fuera capaz de identificar los aspectos de una sonrisa real pero algo le decía que esa persona no era "auténtica". A finales del siglo XIX, un neurólogo francés, Duchenne de Boulogne, realizó una investigación fascinante sobre la sonrisa. Fue capaz de colocar electrodos en el rostro de un hombre y activar en él la misma respuesta "muscular" que una sonrisa. Aunque el hombre estaba utilizando los músculos exactos de una sonrisa, De Boulogne determinó que se trataba de una "sonrisa falsa". ¿Por qué?

Según De Boulogne, cuando alguien sonríe de verdad, se activan dos músculos, el cigomático mayor y el orbicular de los párpados. Duchenne determinó que el orbicular (el músculo alrededor de los ojos) no puede activarse voluntariamente y eso es lo que diferenciaba una sonrisa real de una falsa.

La investigación del doctor Ekman coincidió con la de Duchenne y, aunque estudios recientes indican que es posible llegar a activar ese músculo voluntariamente, en la mayoría de los casos lo que distingue una sonrisa falsa son los ojos. Una sonrisa real es amplia, con ojos estrechos, mejillas elevadas y los párpados inferiores levantados. Se dice que una sonrisa real involucra toda la cara, desde los ojos a la boca, como muestra la figura 5.13.

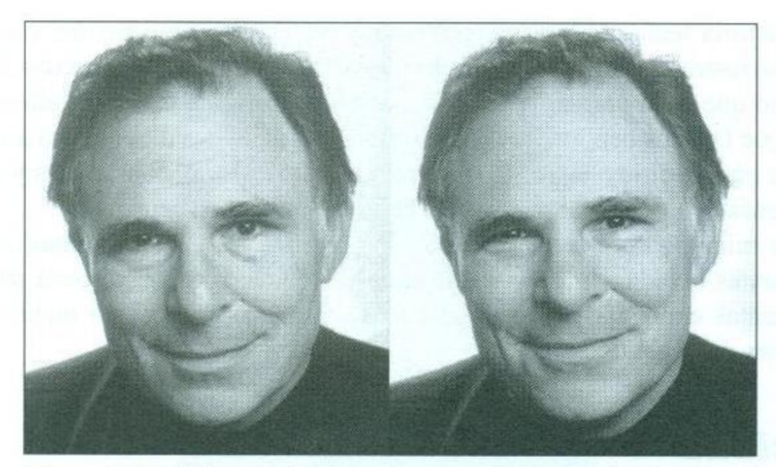


Figura 5.13. *El doctor Ekman muestra una sonrisa falsa (izquierda) junto a una verdadera (derecha).*

Si tapara la parte superior de las imágenes del doctor Ekman, le costaría trabajo determinar cuál es la sonrisa falsa y cuál la verdadera. Cuando examina los ojos es cuando queda claro al ver las dos sonrisas juntas.

Cuando una persona ve una sonrisa real en el rostro de otra, se puede disparar el mismo sentimiento en su interior y provocar que sonría también. Observe la figura 5.14. Este hombre está dando signos de auténtica alegría con una sonrisa real. Observe que todo su rostro está implicado en esa sonrisa.

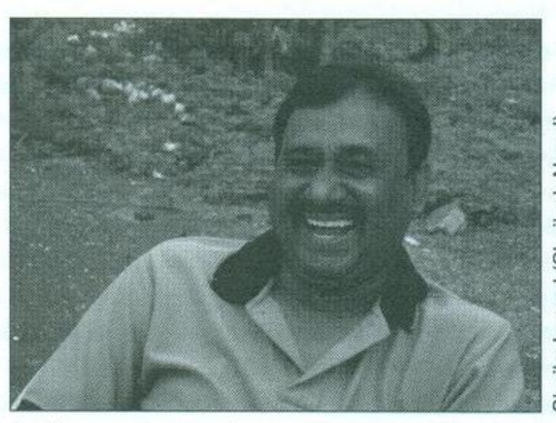


Figura 5.14. *Observe cómo todo su rostro está implicado en su sonrisa.*

Desde el punto de vista del ingeniero social, saber detectar y generar sonrisas auténticas es una habilidad muy valiosa. Es importante que el objetivo se sienta cómodo, para tener un efecto lo más positivo posible sobre él. Los ingenieros

sociales de cualquier clase, ya sean comerciales, profesores o psicólogos, suelen iniciar sus conversaciones con una sonrisa. Rápidamente, el cerebro analiza lo que siente respecto a esa visión, lo cual afecta al resto de la interacción.

En la sección previa se proporciona una gran cantidad de información, pero puede que se esté preguntando cómo puede practicar, no sólo para detectar las microexpresiones, sino también para poder utilizarlas

Cómo prepararse para detectar microexpresiones

En Hollywood siempre se exageran las habilidades de los personajes que aparecen en las películas y en la televisión. Por ejemplo, en la serie de televisión *Lie To Me* (*Miénteme*), basada en el trabajo del doctor Ekman, el protagonista, el doctor Lightman, puede leer microexpresiones sin esfuerzo aparente y, lo que es más sorprendente, en muchas ocasiones puede establecer qué está provocando esas emociones.

En la vida real, gran parte de la investigación que se ha realizado en este campo consiste en sentarse a analizar sesiones pregrabadas fotograma a fotograma. Después de muchos años trabajando en este campo, es probable que el doctor Ekman sea capaz de detectar y analizar microexpresiones muy rápidamente. En los años setenta realizó un proyecto de investigación en el que identificó a ciertas personas que tenían la habilidad natural de detectar y analizar correctamente las microexpresiones.

Ya que la mayoría de nosotros no entramos en esa categoría de quienes tiene una habilidad natural, necesitamos practicar, entrenar y desarrollar nuestra habilidad para leer, realizar y utilizar las microexpresiones. Puedo explicarle lo que me funcionó a mí. Leí los métodos que existen para identificar una microexpresión en particular, después practiqué reproduciéndola delante de un espejo, comparando mi expresión con los apuntes de los expertos que explican cómo se debe realizar. Normalmente utilizaba también una fotografía que mostrara esa emoción porque me ayudaba tener algo que imitar.

Cuando conseguía reproducir la expresión correctamente me centraba en lo que me hacía sentir, haciendo ligeras correcciones en áreas pequeñas hasta que los movimientos musculares me hacían sentir la emoción correspondiente.

Después rastreaba Internet buscando imágenes e intentaba identificar las expresiones de las imágenes. También grababa las noticias o programas de televisión y veía algunas partes a cámara lenta y sin sonido para tratar de determinar la emoción, después volvía a verlo con sonido para comprobar si había acertado. El siguiente paso fue practicar con "sujetos" reales. Observé a la gente interactuando entre sí e intenté identificar las emociones que sentía durante sus conversaciones. Practiqué de dos formas, escuchando la conversación y también sin escucharla.

La razón por la que practiqué de esta forma antes de intentar detectar microexpresiones en mis propias conversaciones es que pensé que resultaría más sencillo hacerlo en una situación real pero en la que no tuviera que preocuparme también en mantener una conversación adecuada. Simplemente leía la expresión facial sin sufrir otras interferencias sensoriales. Utilicé este método antes de conocer al doctor Ekman y sus métodos de entrenamiento. Por supuesto, ha escrito libros con instrucciones que explican paso a paso cómo leer y reproducir estas expresiones. En sus libros aparecen imágenes y ejemplos que muestran esas emociones. Su libro *Emotions Revealed* tiene un formato muy profesional y es excelente para aprender.

En los últimos años el doctor Ekman ha desarrollado y publicado entrenamientos específicos para las microexpresiones. Su sitio Web, `www.paulekman.com`, contiene tres tipos de entrenamiento distintos que han cambiado la forma en que la gente puede aprender esta ciencia tan poderosa.

El entrenamiento de Ekman consiste en una lección para cada microexpresión a través de texto y vídeo. El usuario puede ver el vídeo las veces que necesite para observar la reacción de cada parte del rostro. Después de pasar el tiempo que considere conveniente analizando los vídeos, el usuario puede realizar una prueba previa que le permite comprobar su habilidad para detectar microexpresiones. Cuando hace su elección recibe una confirmación o una corrección. Si es necesaria una corrección, puede pasar a realizar nuevos ejercicios de entrenamiento y formación.

Una vez que el usuario tiene la suficiente confianza en sus habilidades, puede realizar la prueba real. En este caso, no se realizan correcciones. Al usuario se le muestran microexpresiones por un breve periodo de tiempo de una vigésima quinta parte de segundo, debe seleccionar la microexpresión que ha visto y al final de la prueba recibe una puntación.

Con este tipo de herramienta de aprendizaje se pueden necesitar años para llegar a dominar la lectura de las microexpresiones. Una advertencia: el doctor Ekman y sus contemporáneos afirman que, aunque pueda llegar a dominar la lectura de microexpresiones, una microexpresión es limitada. ¿Qué quiere decir esto?

Uno de los trucos que utilizan los actores para mostrar la emoción adecuada en un momento determinado es intentar recordar una situación en la que realmente sintieran la emoción que tratan de retratar; por ejemplo, un momento de felicidad que produjo una sonrisa verdadera. Como ya hemos explicado, es muy difícil imitar una sonrisa verdadera si no se siente auténtica felicidad, pero si puede recordar un momento en el que sintiera esa emoción, sus músculos reaccionarán.

Por lo tanto, aunque pueda llegar a identificar la emoción, lo que no podrá saber es el "porqué" de esa emoción. El "porqué" normalmente se le escapa a la ciencia. Yo conocía a una chica que había tenido algunas malas experiencias de

niña con una persona que se parecía mucho a un buen amigo mío. Cada vez que mi amigo aparecía, ella sufría fuertes reacciones emocionales. Interpretando sus microexpresiones posiblemente se podría ver en su rostro miedo, desprecio e ira. No odiaba a mi amigo, odiaba a la persona que se parecía a él.

Ésta es una idea que conviene recordar cuando interprete microexpresiones. La expresión está relacionada con una emoción, pero no le dice "por qué" aparece esa emoción. Cuando empecé a leer microexpresiones con cierta habilidad, me sentía como un lector de la mente. Sin embargo, la realidad era muy distinta. Hay que tener la precaución de no dar nada por sentado. Puede llegar a ser muy bueno interpretando microexpresiones; no obstante, en secciones posteriores se explica cómo combinar esta habilidad con tácticas de interrogatorio, interpretación del lenguaje corporal y técnicas de obtención de información para, además de descubrir lo que están pensando sus objetivos, conducirlos por el camino que desea.

Puede que todavía se esté preguntando: "¿Cómo puedo utilizar estas habilidades como ingeniero social?".

Cómo utilizan las microexpresiones los ingenieros sociales

Por muy increíble que sea esta investigación y por muy asombrosa que sea la ciencia que hay detrás de esta rama de la psicología, lo que pretendemos con esta sección es aprender a utilizar las microexpresiones en una auditoría de seguridad y también cómo las utilizan los ingenieros sociales malintencionados.

Se explican dos métodos para utilizar las microexpresiones. El primero consiste en utilizarlas para provocar o causar una emoción y el segundo tiene el objetivo de detectar engaños.

Con el primer método utiliza sus propias microexpresiones para provocar una respuesta emocional en el otro. Leí recientemente un artículo que cambió mi punto de vista sobre este tema y me abrió los ojos a un nuevo campo de investigación. Los investigadores Wen Li, Richard E. Zinbarg, Stephan G. Boehm y Ken A. Paller realizaron un estudio llamado *Neural and Behavioral Evidence for Affective Priming from Unconsciously Perceived Emotional Facial Expressions and the Influence of Trait Anxiety* (Evidencia neuronal y de conducta de condicionamiento afectivo a través de expresiones faciales emocionales percibidas inconscientemente y la influencia de los rasgos de ansiedad) que cambiaron la perspectiva de la utilización de las microexpresiones en la ciencia moderna.

Los investigadores conectaron docenas de electrocardiogramas a puntos musculares del rostro de los sujetos. Los aparatos registraban cualquier movimiento muscular en el rostro o en la cabeza. Después, les pusieron unos vídeos en los que

se veían microexpresiones de una vigésima quinta parte de segundo en fotogramas. Los investigadores descubrieron que prácticamente en todos los casos el movimiento muscular de los sujetos imitaba lo que aparecía en el vídeo. Si era miedo o tristeza, los músculos faciales del sujeto registraban esas emociones. Cuando preguntaban a los sujetos por las emociones que estaban sintiendo, coincidían con las emociones que veían en el vídeo.

Esta innovadora investigación prueba que se puede manipular a una persona para que entre en cierto estado emocional exponiéndola a muestras sutiles de esa emoción. He comenzado a investigar en este campo desde el ángulo de la seguridad y lo he denominado "pirateo neurolingüístico", principalmente porque tomo muchos conceptos de las microexpresiones y de la programación neurolingüística (explicada en la sección siguiente) combinándolos para provocar estos estados emocionales en el objetivo.

Imagine esta situación. Un ingeniero social llega a una empresa con la meta de conseguir que la recepcionista inserte una llave USB en su ordenador. Su pretexto es que ha quedado con el director de recursos humanos pero por el camino ha derramado café sobre su currículum. Necesita el trabajo y le pide a la recepcionista que le ayude imprimiendo otra copia del currículum.

Éste es un pretexto sólido que toca el corazón de la recepcionista y que a mí me ha funcionado en el pasado. Sin embargo, si el ingeniero social permite que sus emociones se desaten, puede dar muestras de miedo, que está conectado con el nerviosismo. Ese miedo puede derivar en un sentimiento incómodo en la recepcionista y en el fracaso o rechazo de la petición. Mientras que si es capaz de controlar sus emociones y crear microexpresiones de sutiles muestras de tristeza, que se relaciona directamente con la empatía, entonces tiene bastantes probabilidades de que se atienda su petición. Recuerde la discusión previa sobre los anuncios de televisión que animan a la gente a donar "sólo un euro al día" para alimentar a niños necesitados. Antes de pedir el dinero, antes de anunciar un número de teléfono y una URL, antes de decir que se aceptan tarjetas de crédito, pasan por la pantalla de su televisión largas imágenes de niños muy tristes. Esas imágenes de niños necesitados sufriendo ponen su mente en el estado emocional necesario para que acceda a la petición.

¿Funcionan estos anuncios para todo el mundo? Por supuesto que no. Pero, aunque no todo el mundo hace una donación, sí afecta al estado emocional de la mayoría de la gente. Así es cómo pueden utilizarse plenamente las microexpresiones. Si aprende a exhibir las muestras sutiles de estas microexpresiones, conseguirá que las neuronas de su objetivo imiten el estado emocional que perciben, haciéndolos vulnerables a acceder a sus requerimientos.

Este uso de las microexpresiones puede ser malintencionado, por lo que quiero tomarme un momento para aclarar este punto (véase también el capítulo 9). Saber cómo utilizar las microexpresiones no significa que deba instruir a todo el personal

de una empresa para que se conviertan en expertos en la materia. Lo que significa es que debe llevarse a cabo un buen programa de formación en seguridad. Aunque las peticiones se diseñan para que la gente desee ayudar, salvar o cuidar al otro, las medidas de seguridad deben prevalecer. Será suficiente un sencillo: "Lo siento, no podemos insertar llaves USB ajenas en nuestros ordenadores. Un par de kilómetros más abajo encontrará un centro de reprografía donde le imprimirán un nuevo currículum. ¿Quiere que avise a la señora Smith de que llegará unos minutos más tarde?".

En esa situación, una frase como ésa destroza los planes del ingeniero social a la vez que da al objetivo la sensación de haber sido de ayuda.

Para utilizar las microexpresiones en su máximo potencial, a menudo tendrá que combinarlas con otros aspectos de la conducta humana. El segundo método, cómo detectar los engaños, le explica cómo hacerlo. ¿No sería estupendo hacer una pregunta y saber si la respuesta es verdad o mentira? Este tema ha sido el origen de un debate muy intenso entre profesionales que afirman que los movimientos oculares, el lenguaje corporal, la expresión facial o la combinación de todos ellos pueden distinguir la verdad del engaño. Mientras que hay quienes no creen que esto pueda ocurrir, otros consideran que este método puede utilizarse como una ciencia exacta.

Aunque puede que las dos opiniones tengan parte de razón, ¿cómo puede utilizar las microexpresiones para detectar engaños?

Para responder a esta pregunta debe tener en cuenta varios asuntos además de las microexpresiones porque, como se explica en esta sección, las microexpresiones se basan en emociones y en reacciones a las emociones. Tenga esto en cuenta mientras lee esta sección, que analiza algunas causas y efectos.

Hay cuatro elementos que pueden ayudarle a detectar el engaño en un objetivo:

- Las contradicciones.
- La indecisión.
- Los cambios de actitud.
- La gesticulación con las manos.

En las siguientes secciones tratamos cada uno de estos conceptos en detalle.

Las contradicciones

Las contradicciones pueden dar lugar a confusión porque en ocasiones también tiene lugar en afirmaciones sinceras. Cuando voy a contar una historia a mí se me olvidan a menudo los detalles y necesito que mi mujer me los recuerde. Una vez que me da un par de indicaciones normalmente recuerdo la historia completa. Esto

no significa que siempre que inicio una conversación estoy mintiendo, simplemente no siempre recuerdo todos los detalles con la suficiente claridad como para comentarlos o creo que los recuerdo pero en realidad no es así. Incluso cuando "recuerdo" los detalles, puede que éstos no sean más que mi versión de la realidad y no la forma en que la historia ocurrió de verdad.

Es importante considerar esta deshonestidad involuntaria cuando evalúe las contradicciones como una señal de que alguien miente. Lo que debe provocar una contradicción es que indague más. Una buena manera es observar las microexpresiones mientras le pregunta a alguien sobre esas contradicciones.

Por ejemplo, imagine que ha desarrollado un pretexto en el que es un comercial que realiza una visita. Necesita acceder al director general en persona para entregarle un CD con una oferta especial. Sabe de antemano que el director tiene debilidad por ciertas obras de caridad, por lo que desarrolla su pretexto en base a este dato. Al entrar en el vestíbulo, la recepcionista le dice: "Lo siento, el director no se encuentra en su despacho en estos momentos, puede dejar el CD aquí si lo desea".

Es consciente de que si deja el CD en recepción hay bastantes probabilidades de que nunca se utilice. Además, sabe que el director sí está en la oficina porque ha visto su coche en el aparcamiento y ese día tiene una jornada de trabajo normal. Con esos datos en mente y evitando avergonzar a la recepcionista, dice: "Ah, ¿no está aquí? Le llamé el otro día para preguntarle cuándo podía venir y me dijo que hoy era un buen día. ¿Me habré confundido de día?".

Si ha jugado bien sus cartas y sus expresiones han resultado sinceras, pueden suceder dos cosas:

- Puede que la recepcionista se mantenga firme y diga: "Lo siento, el director no está".
- Puede que se contradiga (lo que quizá sea una indicación de que no está siendo sincera) diciendo: "Deje que compruebe si está en su despacho".

¿Cómo? Ha pasado de un "no se encuentra aquí" a un "deje que lo compruebe". Esta contradicción es señal suficiente de que debe indagar un poco más. ¿Cuáles fueron sus microexpresiones cuando dijo eso? ¿Mostró signos de vergüenza o quizá cierta tristeza por mentir? ¿Se ha enfadado porque la descubrieran mintiendo? ¿Le ha dado vergüenza estar equivocada o se ha sentido confundida? No puede asumir inmediatamente que está mintiendo porque no lo sabe en realidad, puede que no supiera si el director estaba y cuando le ha insistido haya decidido averiguarlo.

Cuando confirme si le director está en la oficina puede indagar un poco más. Nuevamente con el argumento de "a lo mejor me he confundido de día" puede observar sus expresiones faciales para determinar su sinceridad.

Si en el primer intento detectó signos de enfado, seguir preguntando sólo provocará más enfado y vergüenza y la interacción se acabará. En este punto puede decir algo como: "Si el señor Smith no está y me he confundido de día, ¿cuándo puedo encontrarlo en la oficina? ¿Sabe cuándo es el mejor momento?".

Este tipo de preguntas permitirá que ella quede bien y le dará la oportunidad de leer más expresiones faciales. Si no detecta enfado pero sí algo de tristeza o vergüenza puede ser bueno que responda con empatía y comprensión para relajarla: "Habría jurado que me dijo que viniera hoy pero, la verdad, tengo una memoria tan mala que mi mujer siempre me dice que tengo Alzheimer. Me he comprado uno de esos teléfonos *smartphone*, pero no consigo enterarme de cómo funciona. No quiero ser una molestia pero, ¿cuándo puedo venir a entregarle esto? Tengo que asegurarme de entregárselo en persona".

Fíjese bien en las pequeñas contradicciones, pueden ser indicadores clave de un engaño y ayudarle a alcanzar su meta.

La indecisión

Al igual que con la contradicción, se puede utilizar la indecisión para detectar una mentira potencial. Si formula una pregunta que debería responderse rápidamente pero la persona duda un momento, puede ser una indicación de que se está tomando tiempo para inventar una respuesta.

Por ejemplo, cuando mi mujer me pregunta cuánto me han costado mis nuevos artilugios electrónicos, ella sabe que sé la respuesta. La indecisión por mi parte puede significar que estoy evaluando si debo ser sincero o puede que simplemente esté intentando recordar y sumar los precios.

Cuando recibo un informe de situación del colegio de mi hijo en el que dice que ha faltado X días a clase y yo sólo soy consciente de dos o tres ausencias justificadas, le pregunto a qué se deben el resto de faltas. Si la respuesta es: "Papá, ¿no te acuerdas de la cita con el médico y del día que me quedé en casa a ayudarte con un proyecto?", lo más probable es que sea una respuesta sincera porque ha sido rápida y contiene datos comprobables. Sin embargo, si duda y dice algo como: "Vaya, no sé, a lo mejor el informe está equivocado", entonces puede venir bien observar sus microexpresiones durante la respuesta. ¿Indican enfado por haber sido descubierto o tristeza al imaginar el posible castigo? En cualquier caso, debo investigar más y averiguar dónde estaba mi hijo esos días.

Otra táctica a tener en cuenta es cuando antes de contestar la persona repite la pregunta como si estuviera asegurándose de que es correcta. Hacer esto le da tiempo a inventar una respuesta. La utilización de la indecisión para detectar un engaño no es una ciencia exacta pero puede ser un buen indicador. Hay gente que piensa antes de responder. Yo soy de Nueva York, así que hablo rápido. Si alguien

habla más despacio que yo, no significa que me esté engañando. Debe ser capaz de utilizar las microexpresiones para determinar si una persona simplemente habla despacio o si está intentando inventar una respuesta.

Si la emoción que muestra no concuerda con la pregunta formulada, entonces puede que merezca la pena investigar un poco más.

Los cambios de actitud

Durante una conversación puede cambiar la actitud del objetivo cada vez que se aborda un nuevo tema. Puede que detecte un cambio de expresión o en la forma en que se sienta o una clara indecisión. Estas acciones pueden ser indicativas de un engaño. Para comprobarlo, será conveniente profundizar en el tema en cuestión sin levantar sospechas. Estas conductas pueden indicar que la persona está aprovechando el tiempo para inventar la historia, recordar hechos o decidir cuánto quiere contar sobre ese asunto.

La gesticulación con las manos

A menudo, la gente utiliza las manos para ilustrar lo que está diciendo. Por ejemplo, alguien puede utilizar las manos para indicar lo grande que es algo, lo rápido que se mueve o la cantidad de veces que se menciona algún concepto. Muchos profesionales afirman que cuando alguien no está siendo sincero se toca o se frota el rostro varias veces. Existe cierta conexión psicológica entre frotarse el rostro e inventar una historia. Algunas de las pistas utilizadas por los psicólogos y expertos en lenguaje corporal para detectar engaños se explican aquí: `www.examiner.com/mental-health-in-new-orleans/detecting-deception-using-body-language-and-verbal-cues-to-detect-lies`.

Es importante observar cambios en el tamaño, frecuencia o duración de los gestos de las manos. Además, también debe prestar atención a las expresiones faciales que puedan tener algún significado.

Es conveniente tener un plan preparado para responder cuando detecte una mentira. En el anterior escenario de la recepcionista que afirmaba que el director no se encontraba en la oficina, llamar su atención sobre esta mentira seguramente la habría hecho reaccionar avergonzándola y arruinando las opciones de tener éxito. Si su pretexto es alguien con cierta autoridad como un supervisor y sorprende a alguien mintiendo, puede utilizarlo en su provecho. Si "perdona" a esa persona, ésta le deberá un favor. Pero, en el mismo escenario, si su personaje tiene una posición más baja que el objetivo (una secretaria, una recepcionista o un comercial), debe tener cuidado al jugar sus cartas. Una posición autoritaria no encajará con el pretexto.

Al fin y al cabo, todo se reduce simplemente a que como auditor de seguridad debe aprender a utilizar las microexpresiones de la gente para determinar si está mintiendo o diciendo la verdad y si está afectando al objetivo en la forma deseada. En algunos casos incluso podrá utilizar ciertas expresiones para manipular al objetivo hacia un estado mental concreto.

Recuerde: las microexpresiones por sí solas no son suficiente para determinar "por qué" una emoción está teniendo lugar. Detectar que una persona está triste o enfadada no le indicará por qué se siente de esa manera. Cuando utilice las microexpresiones tenga el cuidado de tener en consideración todos los factores en juego para determinar, lo más precisamente posible, la razón de esa emoción.

Los ingenieros sociales maliciosos emplean estas tácticas de utilización de las microexpresiones con metas totalmente diferentes a los auditores de seguridad. Normalmente, no se preocupan de los efectos colaterales en sus víctimas. Si dañar el sistema de creencias de una persona o su estabilidad psicológica o laboral puede darle beneficios, puede estar seguro de que el ingeniero social malintencionado elegirá ese camino.

Previamente ha leído en este libro sobre las estafas que tuvieron lugar tras los ataques del 11 de septiembre sobre Nueva York. La gente que vio la oportunidad de hacer caja a costa de la simpatía de los demás y de la tragedia que ocurrió, no se preocuparon del daño que sus acciones podían causar a otros. Muchos aparecieron de la nada afirmando que habían perdido a familiares en los ataques. Algunas de estas personas malintencionadas recibieron dinero, regalos, apoyo moral e incluso atención mediática para más tarde descubrirse que se trataba de historias falsas.

Las personas de malas intenciones pasan mucho tiempo aprendiendo sobre la gente y sobre lo que les afecta. Este conocimiento hace que sea más fácil localizar una víctima adecuada.

Esta sección sólo ha rozado la superficie del mundo de las microexpresiones; se han llenado volúmenes con el trabajo de muchos profesionales de este campo. Practique hasta leer y emplear con soltura las microexpresiones y verá cómo mejoran sus habilidades comunicativas con los demás. Además, conseguirá mayores éxitos en sus auditorías.

La programación neurolingüística (PNL)

La programación neurolingüística (PNL) estudia el modo en que los humanos piensan y experimentan el mundo que les rodea. Se trata de una materia intrínsicamente controvertida, ya que la estructura de la PNL no conduce a fórmulas precisas ni a datos estadísticos. Muchos científicos discuten y rebaten los principios de la

PNL debido a este hecho, pero su estructura deriva en modelos que explican cómo funcionan esos principios. A partir de estos modelos, se han desarrollado técnicas para cambiar pensamientos, conductas y creencias de forma rápida y efectiva.

Como indica la Wikipedia (fuente: *Oxford English Dictionary*), la programación neurolingüística es "un modelo de comunicación interpersonal interesado principalmente en las relaciones entre patrones exitosos de conducta y las experiencias subjetivas (en especial patrones de pensamiento) subyacentes" y "un sistema de terapia alternativa que pretende educar a las personas en el conocimiento de sí mismas y en una comunicación efectiva para cambiar sus patrones de conducta mental y emocional".

Éste no es en absoluto un libro de autoayuda por lo que, aunque los principios aquí incluidos pueden ayudarle a cambiar algunos patrones de pensamiento consolidados y algunos hábitos, se centra principalmente en cómo puede utilizar la PNL para entender y manipular a quienes le rodean.

Si no está familiarizado con la PNL puede que su primer instinto sea correr a un ordenador y buscar el término en Google. Me gustaría pedirle que no lo haga de momento. Al igual que ocurre con la ingeniería social, lo que encontrará primero serán varios vídeos y demostraciones muy poco realistas, como vídeos de alguien que, tocando el hombro de otra persona, consigue cambiar sus patrones cerebrales y hacerle creer que el color marrón es blanco o algo por el estilo. Estos vídeos hacen pensar que la PNL es una especie de mística y, para quienes desconfían de este tipo de cosas, estos vídeos desacreditan la PNL.

Las siguientes secciones dividen la PNL en varias partes. La primera de ellas contiene una breve historia de la PNL que le ayudará a comprender que sus raíces no residen en la magia callejera; sino que tiene raíces psicológicas profundas.

La historia de la programación neurolingüística

Richard Bandler y John Grinder desarrollaron la programación neurolingüística (PNL) en los años setenta con la ayuda y la orientación de Gregory Bateson. Sus raíces están en la investigación de Bandler y Grinder sobre algunos de los mejores terapeutas del momento.

A partir de la investigación inicial desarrollaron los conceptos "clave" de la PNL. Esta primera investigación derivó en el desarrollo de un "meta-modelo", que reconoce la utilización del lenguaje para influenciar un cambio.

Tanto Bandler como Grinder eran estudiantes de la University of California y utilizaron los principios de su investigación para desarrollar un modelo de terapia llamado meta-modelo. Después de escribir varios libros basados en este modelo,

empezaron a perfeccionar los principios centrales que se convertirían en lo que hoy conocemos como la PNL. Ésta incluye conceptos como el anclaje, la reestructuración, el patrón suizo, el cambio de creencias o las submodalidades.

Después de licenciarse en psicología, Bandler y Grinder comenzaron a organizar seminarios y grupos de prácticas, que les sirvieron para probar y poner en acción los patrones recién descubiertos, a la vez que enseñaban estas técnicas a los participantes. Durante este periodo, se formó un grupo de estudiantes y psicoterapeutas alrededor de Bandler y Grinder que hizo contribuciones valiosas a la PNL, perfeccionándola aún más.

En los últimos años, la PNL se ha convertido en el nuevo término de moda y ha experimentado un rápido crecimiento en número de preparadores, cursos y expertos. Todo el mundo quería aprender a controlar a los demás, mentir sin ser descubierto o resolver todos sus problemas psicológicos y este campo creció sin un cuerpo regulador. Los practicantes de la materia no estaban licenciados y cada grupo enseñaba su propio método de PNL creando certificaciones que les acreditaba como expertos. Todo esto perjudicó la imagen de la PNL.

A pesar de su complicada historia, la PNL puede mejorar sus habilidades como ingeniero social. La siguiente sección explica algunos de los códigos centrales de la PNL.

Los códigos de la programación neurolingüística

A principios de los años setenta, la PNL tenía un código compuesto por el cuerpo de aprendizaje e investigación colectivos que generó el primer libro y el término "programación neurolingüística". Con el paso del tiempo, John Grinder y otros investigadores han seguido contribuyendo al campo de la PNL. El "nuevo código de la PNL" es un marco ético y estético para el desarrollo de la PNL.

El nuevo código de la PNL

Las ideas originales que forman la PNL nacieron en la década de los años setenta. Con el paso del tiempo, John Grinder comprendió que debía cambiarse el antiguo código para adecuarlo a los tiempos modernos. Empezó a trabajar con Gregory Bateson y Judith DeLozier para crear un "nuevo código" que se centraba más en lo que la persona piensa o cree que va a suceder y en cambiar esa creencia. Para lograr ese cambio, es necesario aprender técnicas para poder ampliar las percepciones, superar antiguos patrones de pensamiento y cambiar ciertos hábitos.

El nuevo código se centra en los conceptos clave de los "estados", las "relaciones conscientes/inconscientes" y los "filtros perceptivos", que apuntan a los estados mentales del individuo y a su percepción de esos estados. La intención de estos nuevos conceptos es hacer evolucionar la PNL y ayudar a sus profesionales a pensar en ella de otra forma. Muchos de los principios fundamentales del nuevo código se enseñan hoy en día como parte del programa estándar de PNL. Este nuevo código se entiende mejor con la lectura del libro de Grinder y DeLozier que es una compilación de su seminario "Prerequisites to Personal Genius" (Requisitos previos para el genio personal). Fundamentalmente, el nuevo código establece que para realizar un cambio el cliente debe involucrar su subconsciente, la nueva conducta debe satisfacer su intención positiva original y el cambio debe ocurrir a nivel interno en el estado mental y no a nivel conductual. El nuevo código explica cómo la PNL puede provocar cambios serios y drásticos en el pensamiento de una persona.

Este concepto es clave para la ingeniería social porque cuando comience a investigar y analizar el nuevo código descubrirá cómo puede utilizarse para manipular a las personas. Antes de eso, debe comprender los patrones que utiliza el nuevo código.

Los patrones del nuevo código

La gente suele tener problemas parecidos, por este motivo se han desarrollado grupos de patrones que ayudan a los terapeutas a utilizar la PNL en su práctica profesional. Estos patrones conducen al sujeto a través de una serie de pensamientos hasta un destino deseado. Existen varios libros de calidad sobre los patrones de PNL.

Un ejemplo de patrón sería un plan para aumentar las ventas haciendo que el objetivo hable de sus sueños. Una vez que consigue que hable sobre sus metas y aspiraciones, puede proponer su producto o servicio como una solución perfecta para alcanzar esas metas. Cuando el comprador potencial considera que su producto es adecuado a sus necesidades, se crea en su mente una asociación de su producto con una compra positiva. Si se toma tiempo para buscar en Google esta información comprobará que la PNL es una materia muy extensa y profunda. Puede optar por distintos ángulos y caminos para estudiarla. A pesar de toda la cantidad de información disponible, la pregunta persiste: ¿cómo puede utilizar la PNL un ingeniero social?

Cómo utilizar la PNL

Muchos de los patrones y principios de la PNL conducen a materias como la hipnosis y otras parecidas. Aunque no es buena idea emplear la hipnosis en una auditoría de seguridad, sí puede servirse de muchos de los principios de la PNL. Por ejemplo, puede aprender a utilizar su voz, su lenguaje y la elección de las palabras para guiar a la gente por el camino que desea.

La voz en PNL

Puede utilizar la voz para insertar órdenes en un individuo del mismo modo en que puede utilizar un código para insertar órdenes o comandos en una base de datos de SQL. La inserción sucede por la forma en que dice las cosas; el momento concreto de la inserción se encuadra en una conversación normal. Muchas veces el modo de decir las cosas es más importante que lo que se dice.

La PNL promueve la utilización de órdenes integradas para influenciar al objetivo para que piense o actúe de cierta manera. Además, utilizar los tonos de su voz para enfatizar ciertas palabras de una frase puede provocar que el subconsciente del objetivo se centre en esas palabras.

Por ejemplo, al formular la pregunta: "¿No está de acuerdo?", en lugar de poner el acento en la palabra "acuerdo", como haría normalmente al hacer esta pregunta, quítele el relieve a la palabra haciendo que pierda fuerza al pronunciarla para lograr que la pregunta se parezca más a una orden.

Otra frase muy efectiva es: "Mis clientes normalmente me hacen caso. ¿Quiere que empecemos?". El modo en que se utiliza esta frase y la forma en que está rodeada por otra afirmación consiguen que resulte muy imperativa.

Hablaremos más sobre este tema en la siguiente sección, pero esta técnica por sí sola puede cambiar la forma en que interactúa con los demás; sus principios están profundamente influidos por la PNL.

La estructura de la frase

En el lenguaje hablado, el tono de la voz al final de la frase indica si lo que se está diciendo es una pregunta, una afirmación o una orden. Al formular una pregunta, la voz se eleva al final de la frase. En las afirmaciones, la voz se mantiene constante y en las órdenes la voz decae en el tramo final de la frase.

En los siguientes párrafos, la fuente en **negrita** indica que debe bajar el tono de su voz.

Pruebe este ejercicio. Cuando hace una pregunta como "¿es éste tu perro?", su voz se eleva al final de la frase. No obstante, puede introducir órdenes en las frases simplemente cambiando el punto en el que éstas decaen. Aquí tiene algunas órdenes para practicar. Observe cómo la orden está insertada en la frase.

"¿Recuerdas lo **limpia** que estaba **tu habitación** estas navidades?". La orden insertada es "limpia tu habitación", que se rodea de un desplazamiento temporal a una época feliz como son las navidades. Éste es un ejemplo de una inserción agradable e inofensiva.

"¡**Compre ahora** y verá que todo son **ventajas**!". La frase empieza con un tono de voz bajo, a continuación se eleva a un tono normal para volver a descender al final en "ventajas".

"Muchas de las personas **con** las que **trata mi empresa** suelen ser muy **simpáticas, como vosotros**". Esta frase que incluye un comentario agradable aumenta sus posibilidades de ser contratado, en parte porque al acentuar las palabras adecuadas el oyente escucha la frase **contrata mi empresa**.

Al llevar a cabo una auditoría, puede formar frases al teléfono que maximicen sus probabilidades de éxito, como por ejemplo:

"Soy Larry, del servicio de asistencia; vamos a **dar** una nueva contraseña a los representantes. **Su** nueva **contraseña** es...".

A continuación, encontrará algunos consejos para modular su voz en sus auditorías de seguridad:

- **Practique:** Debe practicar esta manera de hablar para no sonar como un chico entrando en la pubertad. Sus subidas y bajadas de tono no deben sonar artificiales, deben ser sutiles.
- **Sea cuidadoso estructurando la frase:** Elabore frases que potencien su habilidad para lograr su meta. No sea excesivamente directo. Una orden como: "Déjeme pasar al cuarto del servidor ahora mismo" probablemente no funcionará, pero puede utilizar estas técnicas vocales para lograr que el objetivo esté más dispuesto a aceptar esa idea.
- **Sea realista:** No pretenda que la gente caiga rendida a sus pies en cuanto diga cualquier cosa. Lo que hacen estas técnicas es situar a su objetivo en posición para que sea más fácil que logre lo que quiere de ellos.

Existe una técnica llamada *Ultimate Voice* (La voz definitiva) que, si se domina, obtiene muy buenos resultados. En cierta ocasión, entrevisté en un *podcast* a un profesional de la PNL que tenía este don. Cuando hablaba daba la sensación de que era imposible discutir con él. Hablaba con tanto control y técnica que no se me pasaba por la cabeza estar en desacuerdo con lo que decía. ¿Cómo puede dominarse esta técnica?

Utilizar la voz definitiva

Puede llegar a dominar el uso de la voz definitiva, pero debe practicar mucho. La habilidad de insertar órdenes en una conversación normal es muy útil cuando se domina. La voz definitiva es la habilidad de introducir órdenes en la mente de la gente sin que se percate de ello. Al intentarlo, puede resultar muy artificial, hasta que practica lo suficiente como para sonar natural.

Los hipnotizadores utilizan esta técnica muy a menudo, como por ejemplo:

"Puede sentir como **se va relajando** mientras se desliza a una profunda **calma**".

Esta frase estándar utilizada habitualmente en terapia puede adaptarse para incluir prácticamente cualquier orden que quiera. Ponga un énfasis especial en las vocales de las palabras que quiere acentuar (por ejemplo: "seee vaaa reeela-aajaaandooo").

En *Planet NPL* (`www.planetnlp.com/`) encontrará tres ejercicios que puede practicar para dominar esta técnica.

1. **Desplace su voz:** Presione sus manos contra su nariz y diga "nariz". Concéntrese en su nariz mientras repite la palabra hasta que pueda sentirla vibrar. Realice el mismo ejercicio con las manos sobre la garganta diciendo "garganta". Vuelva a hacerlo con las manos sobre el pecho diciendo "pecho". Practique hasta que realmente pueda sentir la vibración en cada lugar. Observe las diferencias de cada sonido.

2. **Utilice los registros:** Diga "a" empezando en una nota alta. Manteniendo la boca abierta, deje que la nota vaya bajando hasta que se quede sin aliento.

   Repita el ejercicio diez veces.

   Después, empezando en una nota baja, diga "u" y suba de nota hasta su máxima capacidad.

   Repita el ejercicio diez veces.

3. **Practique la resonancia:** Para utilizar su voz correctamente, ésta debe modularse con el aparato de resonancia, que se sitúa en el área alrededor de la nariz y la boca.

   Existen dos formas de practicar la resonancia:

   - Pronuncie "mmmmmmm" en el tono que más le convenga, seguido inmediatamente por la palabra "radio". Realice este ejercicio varias veces y después pruebe con las palabras "no", "uno", "dos" y "tres".

   - Pronuncie "mmmmmmm" y deje que sus labios vibren. Debe intentar sonar como una paloma. Suba y baje el tono de voz. Esto le resultará complicado si tiene tensión en la mandíbula o en el rostro. Cuando lo haga correctamente durante unos minutos, notará que se le entumece el rostro.

Al cabo de un momento utilizando estos métodos, observará que su voz suena más enérgica. Si no lo percibe, grabe su voz y escúchela después para comprobar cómo suena. La mejor manera de mejorar es practicar estos ejercicios durante cinco minutos al día.

La práctica le ayudará a controlar esta técnica vocal. Por ejemplo, normalmente soy una persona que habla muy alto. Parece que soy incapaz de susurrar. Necesito practicar mucho para controlar mi tono de voz y mi volumen. Realizar ejercicios sencillos como éstos ayuda a controlar las características de su voz.

Cuando quiere introducir una orden oculta en una frase bajando el tono de voz, es fundamental llevarlo a cabo con la sutileza suficiente para que el objetivo no se dé cuenta. De lo contrario, se activará una alarma en su subconsciente indicándole que sucede algo raro. Si esto sucede, percibirá lo que está intentando hacer y se cerrará en banda.

Como en el resto de áreas de la ingeniería social, si la habilidad no surge de forma natural, la práctica es fundamental. Intente esta técnica vocal con sus familiares y amigos antes de llevarla a cabo en una auditoría de seguridad.

En mi experiencia personal, cuando empecé a utilizar las técnicas de la voz definitiva, decidí que mi meta era introducir órdenes en las preguntas. Tardé mucho en conseguirlo pero lo logré probando frases sencillas como:

"Cariño, ¿qué **quieres cenar** esta noche, **filete** o alguna otra cosa?".

Para terminar esta sección, considere estas tres cosas en las que debe centrarse cuando estudie la PNL:

- **Tonos de voz:** Como ya hemos explicado, el tono de su voz, así como el énfasis que ponga en ciertas palabras, puede cambiar por completo el significado de una frase. Utilizando el tono y el énfasis puede introducir órdenes en el subconsciente del objetivo logrando que sea más vulnerable a la sugestión.
- **Elija sus palabras con cuidado:** Aprenda a elegir las palabras que tengan un mayor impacto. Utilice palabras positivas cuando quiera que el objetivo asocie un pensamiento positivo a esas palabras y palabras negativas cuando pretenda lo contrario. Esta técnica también le ayudará a conseguir que su objetivo sea más maleable.
- **Elabore una lista de frases imperativas que pueda utilizar en persona o al teléfono durante una auditoría de seguridad:** Escribir y practicar frases imperativas le ayudará a recordarlas y utilizarlas cuando las necesite.

Ante todo, practique. Controlar los tonos de su voz, las palabras que elige y la manera de pronunciarlas no es una tarea sencilla. Practicar puede hacer que lo consiga de forma más instintiva.

La PNL es una materia poderosa y, al igual que con las microexpresiones, sólo hemos rozado la superficie. Una vez que empiece a dominar las técnicas de PNL y la habilidad para leer expresiones faciales, el siguiente paso lógico es utilizar estas herramientas cuando interactúe con un objetivo. A continuación, pasamos a analizar las tácticas que utilizan los profesionales en los interrogatorios.

Entrevistas e interrogatorios

Escenario 1: La puerta se abre, el sospechoso está visiblemente nervioso. El capitán malhumorado aparece, le agarra por el cuello de la camisa y lo lanza contra la pared. Manteniéndose a dos centímetros de su cara, le grita: "¡Me vas a decir lo que quiero saber, por las buenas o por las malas!".

Escenario 2: El chico malo está atado a una silla, magullado tras la paliza recibida. El interrogador coge unos alicates y dice: "Vas a empezar a hablar en un momento...".

Escenario 3: El sospechoso está sentado en una silla y entran en el cuarto dos oficiales de policía. Tranquilamente, se acercan a la mesa donde dejan una carpeta etiquetada con la palabra "pruebas". Antes de sentarse preguntan: "¿Quieres un refresco, un café o algo?".

El primer oficial abre una bebida fría y dice: "Gracias por haber venido para ayudarnos...".

¿Cuál de estos escenarios es una escena de un interrogatorio real? Si cree que es el tercero, está en lo cierto. Ésa es la forma en que discurre normalmente un interrogatorio. Las dos primeras situaciones se han retratado tantas veces en las películas y en las series de televisión que mucha gente cree que son reales. Situaciones de guerra y países que no prohíben el uso de la tortura aparte, el tercer escenario representa la forma en que habitualmente empiezan los interrogatorios.

Sin embargo, como ingeniero social raramente se encontrará en una situación en la que su objetivo le esté esperando en una habitación para que le interrogue. Teniendo esto en cuenta, se preguntará cómo puede utilizar las tácticas de los interrogadores y entrevistadores profesionales. Antes de continuar, debe comprender las diferencias entre un interrogatorio y una entrevista. La siguiente tabla muestra algunas de estas diferencias, pero este tema tiene distintos puntos de vista, ángulos y opiniones, por lo que puede haber algunas más.

Entrevista	Interrogatorio
El sujeto habla, usted escucha	Usted le habla al sujeto sobre sus declaraciones.
El sujeto dirige la conversación; usted aclara sus afirmaciones y escucha, después aplica las habilidades de la PNL	Usted dirige la conversación. Aplica las técnicas de la PNL en este momento.
No acusatoria	Acusatorio.
De naturaleza suave	De naturaleza dura.
El sujeto está cómodo y en el emplazamiento que ha elegido	El sujeto está tenso en un cuarto de interrogatorios.

Entrevista	Interrogatorio
Usted reúne información (quién, qué, cuándo, dónde, por qué y cómo)	Si revela cierta información, puede descubrir detalles.
Al principio de la investigación	Última sesión para conseguir respuestas.

La diferencia principal entre una entrevista y un interrogatorio es que la entrevista se realiza en un ambiente en el que el objetivo está cómodo física y psicológicamente, mientras que en el interrogatorio la idea es presionar al objetivo haciéndole sentir incómodo con el emplazamiento y las preguntas formuladas para que confiese o revele algún conocimiento que posee.

Interrogar bien es un arte que se domina a través de la experiencia. Muchas de las habilidades de la ingeniería social están relacionadas con esta técnica. Habilidades como las maniobras de obtención de información (véase el capítulo 3), leer los rostros y los gestos de la gente y comprender la conducta humana pueden ayudarle a ser realmente bueno interrogando a sus objetivos.

La habilidad de entrevistar correctamente a sus objetivos es muy útil pero, si domina las maniobras de obtención de información, será un maestro haciendo entrevistas.

Los principios para interrogar correctamente se utilizan ampliamente por los mejores auditores profesionales. La mayoría de ellos considera que es importante dedicar un tiempo considerable a dominar las técnicas para colocar a un objetivo en una situación de desasosiego físico o psicológico que ayude a sonsacarle información con más facilidad.

Tácticas profesionales de interrogatorio

Antes de realizar un interrogatorio o una entrevista, es necesario haber procedido a una recopilación de información. Debe obtener toda la información posible sobre el objetivo, la empresa, la situación y todos los detalles que rodean a estos elementos. Debe saber cómo abordar a un objetivo y qué decirle y tener en mente el camino que va a tomar con él. Preste atención al entorno y a los posibles cambios en el objetivo durante el primer acercamiento y la conversación.

Uno de los errores más comunes en las personas que se inician en los interrogatorios y las entrevistas es asumir que cualquier cambio en la conducta tiene una gran importancia. El hecho de que el objetivo se cruce de brazos no significa que esté experimentando un pensamiento cerrado; puede que tenga frío, que tenga un problema de olor corporal o que esté acusando el estrés debido a sus preguntas.

No tenga en cuenta un solo signo; fíjese en grupos de signos. Por ejemplo, un objetivo cruza los brazos, gira la cabeza y apoya los dos pies firmemente en el suelo. Esta persona se ha cerrado; en otras palabras, su lenguaje corporal indica que no va a revelar más información ni va a cooperar más, se ha cerrado al exterior. Lo más importante es observar los grupos de cambios y tomar nota del tema que se está tratando cuando esos cambios tienen lugar.

Éstas son algunas áreas que se deben observar en busca de cambios al iniciar una entrevista o un interrogatorio:

- **La postura corporal:** Erguido, abatido, ladeado.
- **El color de piel:** Pálido, enrojecido, blanco, cambios de color.
- **La posición de la cabeza:** Erguida, inclinada, hacia delante/atrás.
- **Los ojos:** Dirección, apertura.
- **Las manos y los pies:** Movimiento, posición, color.
- **Boca/labios:** Posición, color, inclinación hacia arriba/abajo.
- **Sentido preferencial:** Visual, auditivo, cinestésico.
- **Voz:** Tono, ritmo, cambios.
- **Palabras:** Cortas, largas, número de sílabas, disfunciones, pausas.

Los cambios pueden indicar que debe prestarse atención a una pregunta o línea de cuestionario. Por ejemplo, si la postura corporal es relajada antes de preguntar: "¿Está el director general? Tengo que entregarle esta información para que la revise", y en ese momento la postura cambia y se vuelve defensiva (el torso girado y los ojos evitando mirarle), puede ser un indicador de que el objetivo se dispone a decir algo incierto, por lo que es necesario continuar el cuestionario para descubrir la verdad sobre este asunto.

Preste especial atención a las palabras que utiliza el objetivo. Fíjese en su voz y en el modo en que contesta las preguntas durante el proceso. Cuando formula una pregunta, ¿cuánto tiempo tarda en contestar? Si responde muy rápido puede ser signo de ser una respuesta ensayada. Si se toma demasiado tiempo puede que se esté inventando la respuesta. El tiempo de respuesta cambia en cada persona, por lo que debe ser capaz de determinar cuál es la pauta "natural" de su interlocutor.

En una actuación de ingeniería social, es importante establecer rápidamente cuáles son las reacciones naturales del objetivo (lo que podríamos denominar sus valores de referencia). La clave del éxito en esta faceta está en ser muy observador. Un método efectivo para establecer los valores de referencia del objetivo consiste en formular preguntas que le obliguen a acceder a distintas partes de su cerebro.

Se realizan preguntas inofensivas que requieren un ejercicio de memoria simple y preguntas que requieren la utilización del pensamiento creativo. Entonces, deben observarse manifestaciones externas de la activación de la memoria, tales como las microexpresiones y las señales corporales.

Otra área a la que prestar atención son los cambios en el tiempo verbal y en la utilización de pronombres. Los cambios en el tiempo verbal de pasado a futuro pueden ser señales que merece la pena investigar más a fondo. Cambiar de tiempo verbal puede indicar un engaño. Cuando el objetivo cambia el tiempo verbal puede ser una indicación de que está inventando la respuesta o de que está pensando en una afirmación anterior para elaborar su respuesta. Continuar investigando puede revelar la verdad en estos casos. También deben vigilarse los cambios en el tono y la velocidad de la voz (¿están aumentando con el estrés?).

No es necesario que aprenda todas estas técnicas al mismo tiempo. Cuanto más practique escuchando y observando a la gente, más sencillo le resultará hacerlo sin tener que pensar. Los interrogatorios profesionales están compuestos por varias partes. Las siguientes secciones explican cada una de esas partes en el contexto que concierne a un auditor profesional.

La confrontación positiva

En la terminología de las fuerzas del orden, la "confrontación positiva" no se refiere a algo bueno o positivo; al contrario, significa que el agente le está explicando al sospechoso que él es quien ha cometido el crimen; en otras palabras, el agente está realizando una acusación directa. En una auditoría de seguridad, el proceso es un poco diferente porque ya ha identificado al "objetivo" y lo que va a hacer a continuación es decirle (posiblemente utilizando las tácticas de PNL mencionadas previamente) que va a hacer lo que le pide.

Se enfrenta al objetivo con la intención de situarle en disposición de hacer lo que desea. Por ejemplo, puede acercarse a una recepcionista y preguntar: "¿Está el señor director? He quedado para reunirme con él". O, utilizando la confrontación positiva, puede decir: "Vengo para mi reunión de las 11 con el señor director". Observe que en la segunda frase se afirma que la reunión está concertada, se da por hecho que el director le espera y lo expresa de forma que muestra estar seguro de que la reunión se va a celebrar.

El desarrollo del tema

En los interrogatorios policiales el desarrollo del tema tiene lugar cuando el interrogador elabora la teoría por la que considera que el sospechoso es culpable del delito. Muchas veces se transmite esa teoría al sospechoso durante el interro-

gatorio. "Así que te insultó, perdiste el control y cogiste la barra y empezaste a golpear el parabrisas". Mientras el agente cuenta la historia, él o un compañero observa el lenguaje corporal y las microexpresiones del sospechoso en busca de signos que indiquen que la teoría es cierta.

Aunque este método puede utilizarse en ingeniería social, es importante señalar que el desarrollo del tema necesita que intente ver su pretexto desde el punto de vista del objetivo. ¿Qué aspecto tendrá, qué dirá y cómo actuará un "técnico de asistencia", un "gerente" o un "compañero de trabajo"?

En ingeniería social el desarrollo del tema tiene lugar cuando las evidencias que expone sirven de apoyo al tema del pretexto que representa. Normalmente, siempre que aborda a un objetivo, en persona o por teléfono, está desarrollando un pretexto de algún tipo. Este pretexto, como es lógico, apoya su argumento o tema. En esta parte del interrogatorio es cuando expone razones o argumentos para apoyar el pretexto (véase el capítulo 4 para poder recordar los conceptos del pretexto).

Por ejemplo, en una auditoría que realicé, mi pretexto era muy sencillo, era un empleado de la empresa. Cogí una publicación comercial que encontré en la papelera y seguí a un grupo de empleados para cruzar la puerta con ellos. Cuando nos acercamos al guardia de seguridad, inicié una conversación muy sencilla con uno de los empleados sobre un artículo de la revista. Todas mis acciones colaboraron al desarrollo del tema. La meta era darle a la persona que normalmente me detendría una justificación para no hacerlo.

Cuanto más se integre, menos destacará y más sencillo será que los guardias de seguridad tengan un motivo para no detenerle y dejarle entrar.

Manejar los rechazos y sobreponerse a las objeciones

Ya sea al teléfono o en persona, ¿cuál es su plan de acción si se le niega el acceso a la información o al lugar que pretende? Me gusta llamar a estas situaciones barreras de la conversación. La gente las utiliza continuamente con los comerciales: "No estoy interesado", "Ahora no tengo tiempo", "En este momento estaba saliendo por la puerta...".

Sea cual sea el tipo de barrera que el objetivo utilice, debe tener un plan para superarla y manejar la negación de acceso. A mí me gusta descartar las objeciones de antemano si percibo que la situación lo justifica.

Cuando trabajaba en ventas tenía un compañero llamado Tony cuya táctica consistía en llamar a la puerta, presentarse y decir enseguida: "Comprendo que quiera decirme que no está interesado pero, antes de que lo haga, déjeme preguntarle algo: ¿valen cinco minutos de su tiempo 500 euros?".

En ese momento, era mucho más improbable que la persona dijera: "No estoy interesada". Al reducir las posibilidades de rechazo y continuar con una pregunta, Tony conseguía que el objetivo pensara en algo distinto a la objeción que iba a poner.

Está claro que en una actuación de ingeniería social no puede acercarse a un guardia de seguridad y decir: "Ya sé que no quiere dejar pasar a desconocidos pero..." porque levantaría demasiadas sospechas. En las auditorías de seguridad la metodología para superar objeciones es mucho más compleja.

Debe pensar en el tipo de objeciones que pueden surgir y organizar su argumento, su historia, su vestimenta y su aspecto para anticiparse a ellas. Además, debe tener preparadas unas buenas respuestas por si surgen objeciones. No puede irse sin más o colgar el teléfono. Una estrategia de retirada correcta le da la opción de volver al ataque más adelante.

Una estrategia de retirada puede ser tan sencilla como decir: "Bueno, señora, siento que no me deje pasar a ver al señor Smith. Sé que se sentirá decepcionado porque estaba esperando mi visita, pero le llamaré más tarde para concertar una nueva cita".

Mantener la atención del objetivo

Si ha manejado sus armas correctamente y se encuentra frente a su objetivo, puede que éste empiece a pensar en qué pasaría si no le permite acceder, coger el archivo o hacer lo que pretende. Debe sacar provecho de ese miedo inherente y utilizarlo para continuar moviendo al objetivo hacia su meta.

Algunas frases cortas como: "Gracias por su ayuda. Estaba tan nervioso por esta entrevista que he debido marcar mal la fecha en el calendario. Espero que la señora directora de recursos humanos esté en un sitio más cálido que éste", dan pie a una respuesta con la que puede continuar: "Quiero darle las gracias por su ayuda. ¿Cuándo estará de vuelta para que pueda concertar otra cita?".

Presentar una ruta alternativa

Cuando esté interrogando a su objetivo en una auditoría puede que su plan original no sea recibido con sonrisas, por lo que es buena idea tener preparado un plan de acción alternativo igual de efectivo.

Puede que ya haya probado todas las tácticas posibles con Sally, la recepcionista, para que le deje ver al señor Smith. Todas las tácticas han fallado y se le ha denegado el acceso. Debe tener una ruta alternativa preparada, como por ejemplo: "Sally, entiendo que tiene que asegurarse de que todas las visitas sean con cita previa. El problema es que no sé cuándo voy a volver a estar por la zona. ¿Puedo dejarle este CD con información para el señor Smith y le llamo más tarde para ver si concertamos una cita?".

Debe tener varios CD preparados con documentos PDF con código malicioso para que esta nueva ruta sea exitosa. También es importante haber practicado previamente y haber utilizado con rapidez las tácticas de interrogatorio.

Un contacto me envió un documento titulado "Entrevistas e interrogatorios", que utiliza el Departamento de Defensa para entrenar a su personal para que supere la prueba del polígrafo. Señala las distintas técnicas que utilizan los interrogadores profesionales y que muestro a continuación. Estudiándolas se puede aprender mucho sobre los distintos métodos que pueden utilizarse en ingeniería social.

- **Enfoque directo:** En este enfoque, el interrogador asume un aire de confianza. La actitud y las maneras del interrogador dan a entender que descarta la opción de que el sospechoso sea inocente. Sin amenazarle, desarma al sospechoso diciéndole que cualquier persona en su lugar habría hecho lo mismo que él.

  Como ingeniero social puede utilizar este enfoque dependiendo del pretexto que esté desarrollando. Puede que sea un supervisor, un consultor u otra persona que tenga cierto poder sobre el objetivo. Esto significa que debe adoptar un aire de confianza y dar por sentado que el objetivo le "debe" la respuesta que solicita.

- **Enfoque indirecto:** Se permite al sospechoso contar su versión de los hechos en detalle y el interrogador busca omisiones, discrepancias y distorsiones. El trabajo del interrogador consiste en hacer ver al sospechoso que lo mejor que puede hacer es decir la verdad.

  Este enfoque puede utilizarse en una auditoría de seguridad abordando al objetivo con una pregunta diseñada para sonsacarle información, en lugar de interpretando un papel. Puede obtener la información que quiere dejando hablar al objetivo.

- **Enfoque comprensivo:** El manual del Departamento de Defensa ofrece ideas excelentes sobre este enfoque. El interrogador baja la voz y habla en un tono suave y tranquilo, dando la impresión de que es una persona comprensiva. Se sienta junto al sospechoso e incluso puede que ponga la mano sobre su hombro o le dé unas palmaditas en el brazo. El contacto físico en el momento apropiado es muy efectivo.

  El auditor profesional puede utilizar este enfoque del mismo modo. Puede que escuche a unos empleados quejarse de su jefe. O puede que siga al objetivo hasta un bar y entable con él una conversación en la que se muestre comprensivo con alguna situación. Puede utilizar este enfoque de muchas maneras y suele ser muy efectivo.

- **Enfoque emocional:** Este enfoque se aprovecha de la moralidad y las emociones del sospechoso. En esta táctica se utilizan preguntas como por ejemplo: "¿Qué pensarían tu mujer y tus hijos de esto?". Los pensamientos que se despiertan emocionalmente le disgustan y le ponen nervioso; cuando esas emociones se ponen de manifiesto el interrogador puede sacar partido de ellas.

  Puede utilizar este enfoque aprovechando una debilidad de su objetivo. En una auditoría que realicé sabía que al objetivo le gustaba participar en obras benéficas para niños con cáncer. Utilizando esos sentimientos logré que realizara cierta acción que de otra forma no hubiera hecho.

- **Enfoque lógico:** Este enfoque deja de lado la parte emocional y se centra en presentar pruebas concluyentes de culpabilidad. El interrogador se sienta muy erguido y adopta una conducta de hombre de negocios, mostrando mucha confianza.

  En ingeniería social puede valerse de este enfoque cuando presente pruebas de su razones legítimas para estar presente en un sitio determinado, por ejemplo cuando está vestido y equipado como un técnico de asistencia y debe mostrarse con el aire de confianza necesario para hacer ver que todo está en orden.

- **Enfoque agresivo:** Para el interrogador existe una línea muy fina que no debe cruzarse, entre recopilar información e infringir los derechos del objetivo. En este enfoque, se alza la voz y se actúa de forma agresiva, pero nunca deben violarse los derechos civiles del sospechoso.

  Debe recordar esta fina línea cuando utilice este enfoque en una auditoría de seguridad. Recuerde el caso de Hewlett-Packard, explicado en el capítulo 4. Que le hayan contratado para un trabajo de ingeniería social no le da derecho a violar las leyes civiles. Normalmente, las empresas que le contraten no le autorizarán para pinchar teléfonos privados, leer correos electrónicos personales o invadir la privacidad de las personas.

- **Enfoque combinado:** Un interrogador puede combinar dos enfoques para lograr mejores resultados. Esta decisión se toma en base a la personalidad del sospechoso.

  La combinación de enfoques puede ser útil en una auditoría de seguridad. Por ejemplo, después de descubrir algunos detalles personales de su objetivo (como su bar favorito) puede acercarse a él iniciar una conversación. Esta táctica, sobre todo si se emplea en un ambiente relajado, puede dar muy buenos resultados abriendo a la gente.

- **Mostrar indiferencia:** Este enfoque es muy interesante ya que el interrogador actúa como si no le interesara la confesión porque considera que el caso ya está resuelto. En ese momento, puede manipular al sospechoso para que explique su versión de los hechos.

  En ingeniería social puede utilizar este enfoque en el caso de que sea descubierto en un lugar o una situación en la que no debería estar. Puede mostrar indiferencia en lugar de miedo por haber sido descubierto. Al mostrarse indiferente puede hacer que la persona que le ha descubierto no se alarme demasiado y le da la oportunidad de disipar las preocupaciones. Kevin Mitnick (véase el capítulo 8 para más información sobre Mitnick) era un maestro utilizando esta táctica. Tenía la habilidad de pensar muy rápido y conseguía escapar de situaciones muy complicadas.

- **Proporcionar una justificación:** El interrogador justifica la infracción o delito, haciendo que el sospechoso se relaje y dándole una excusa para confesar pensando que sale bien parado de la situación. El interrogador debe tener cuidado para no utilizar una excusa tan buena que el sospechoso pueda utilizarla como defensa en un juicio.

  En ingeniería social, sin embargo, sí se debe utilizar la mejor excusa posible, de forma que el objetivo no tenga que pensar antes de justificar su acción y acceder a lo que le pide.

  Una forma de utilizar este enfoque es explicar que una persona de alto cargo le ha pedido que esté ahí. Puede apoyar este argumento diciendo: "Entiendo cómo se debe sentir pero no quiero ni imaginarme lo defraudado que se va a sentir el señor Smith si el lunes cuando vuelva no está arreglado el problema con los correos electrónicos". Este argumento le da al objetivo una justificación para hacer lo que le pide.

- **Enfoque egotista:** Este enfoque se centra en el orgullo. Para que funcione, necesita un objetivo que se sienta orgulloso de algún logro. Alabando su aspecto, su inteligencia o el modo en que se cometió el crimen, se puede tocar su ego como para que desee confesar y demostrar que, es así de listo.

  Este método se utiliza mucho en ingeniería social. Al elogiar los logros de alguien se consigue que revele sus más íntimos secretos. En el caso del ingeniero nuclear de visita en China (véase el capítulo 3), lo agasajaron con cumplidos y halagos hasta que finalmente reveló una información que debería haber mantenido en secreto.

- **Exageración:** Si el interrogador exagera los hechos del caso, puede lograr que el sospechoso admita sólo la parte que es real. Un ejemplo sería si un interrogador acusa a un ladrón de haber intentado cometer una violación

y le dice: "¿Qué otro motivo podría tener alguien para entrar en una habitación en plena noche?". A menudo, la reacción será que el sospechoso admita que pretendía robar y no cometer una violación.

Puede utilizar este método exagerando la tarea que pretende llevar a cabo. Exagerando el motivo por el que está ahí, puede conseguir que el objetivo le dé un acceso menor. Por ejemplo, puede decir: "El señor Smith me pidió que arreglara su ordenador personalmente porque ha perdido mucha información, pero si no le parece bien, creo que podría solucionar su problema desde otro ordenador de la oficina".

- **Desmontar la coartada:** Raramente un sospechoso confiesa su delito de golpe a la primera. Esta táctica consiste en que vaya admitiendo pequeños detalles, como que efectivamente estaba en el lugar de los hechos, que es el dueño del arma o que tiene un coche parecido, consiguiendo de esta forma que vaya admitiendo cada vez más hechos hasta lograr finalmente una confesión completa.

  En una auditoría de seguridad puede que le detengan en la puerta y el guardia le deniegue el acceso al edificio. Puede intentar entrar con una frase como ésta: "Comprendo que el señor Smith esté ocupado y no pueda recibirme. ¿Le importaría hacerle llegar este CD con información sobre nuestros productos y yo le llamo mañana por teléfono para hablar de ello?".

  Es un acceso menor, pero si no consigue entrar, al menos deja su CD en la puerta.

La meta final

Para prepararse para utilizar tácticas adecuadas de entrevista e interrogatorio puede que necesite dar respuesta a una serie de preguntas. Le animo a que las escriba en un cuaderno, porque eso le ayudará a preparar su encuentro con el objetivo. Además, al escribir las respuestas las hace reales y le proporciona una base sobre la que trabajar durante la preparación del interrogatorio.

Conteste a estas preguntas:

- **Quién:** ¿Con quién se va a desarrollar el encuentro? ¿Cuál es su papel? Haga una lista de nombres, títulos y otros datos relevantes para el interrogatorio.
- **Qué:** Exactamente, ¿qué preparación se ha llevado a cabo y cuál es su meta durante el interrogatorio? Debe definir sus aspiraciones.
- **Cuándo:** ¿En qué momento va a tener lugar el interrogatorio? ¿A qué hora del día o de la noche? ¿Cuáles son las circunstancias que han llevado a decidir ese horario? ¿Se ha enterado de que se va a celebrar una fiesta?

¿Ha elegido un momento en el que la mayoría de los empleados están de vacaciones? ¿Va a ser en la hora del almuerzo? ¿Va a llevarse a cabo durante el relevo del personal de seguridad?

- **Dónde:** ¿En qué lugar va a realizarse el interrogatorio? ¿Va a ser en la ubicación del objetivo? ¿Va a seguir al objetivo hasta su gimnasio, el bar o la guardería? ¿Cuál es el mejor lugar para intentar obtener la información del objetivo?
- **Por qué:** La gente ya escucha este pregunta lo suficiente de sus hijos, pero aun así hay que hacerla. ¿Cuál es el motivo de este interrogatorio? ¿Conseguir que el objetivo admita la ubicación de algo? ¿Lograr que revele información que no debería revelar? ¿Obtener acceso a un cuarto o a un servidor?
- **Cómo:** ¿Qué métodos va a utilizar en este interrogatorio? ¿La PNL? ¿Órdenes insertadas? ¿El desbordamiento de búfer humano (explicado al final de este capítulo)? ¿Microexpresiones?

Por supuesto, en un interrogatorio policial, la meta es lograr la confesión de un delito. En ingeniería social, la meta es una confesión de otro tipo. Debe conseguir que la gente se sienta cómoda revelándole información, lo cual puede lograrse utilizando las tácticas de interrogatorio explicadas previamente. Una vez que domine estas tácticas, sus interrogatorios deben parecer entrevistas fluidas y suaves. No obstante, existen otras técnicas que puede emplear cuando interrogue o entreviste a sus objetivos.

La gesticulación

Existe una gran variedad de gestos debido al hecho de que dependen en gran medida de los orígenes culturales. Al contrario que las microexpresiones, que son universales, los gestos habituales en un país pueden resultar ofensivos o no tener ningún significado en otro.

Aquí tiene un ejercicio para ayudarle a entender las diferencias gestuales. Si lo desea escriba sus respuestas para consultarlas en unos minutos. Dependiendo de la cultura de la que proceda, será interesante comprobar los resultados.

Escriba lo que cree que significa este gesto e indique en cada caso si lo considera grosero:

1. Mantener la palma de la mano hacia arriba, señalar a alguien con el dedo índice y llamarlo por señas.

2. Hacer el signo de la "V" con el dedo índice y corazón.
3. Sentarse mostrando la planta de los pies.
4. Hacer el signo de "ok" con los dedos.
5. Agitar la mano con la palma hacia fuera.
6. Mover la cabeza arriba y abajo.

Si ha escrito sus respuestas, compárelas con estos interesantes datos relativos a diferencias culturales:

1. En Estados Unidos este gesto simplemente significa "ven aquí", pero en Oriente Medio y en el Lejano Oriente, en Portugal, España, Latinoamérica, Japón, Indonesia y Hong Kong, llamar a alguien de esta manera se considera grosero o incluso ofensivo. En algunos de estos países resulta más aceptable llamar a alguien con la palma de la mano hacia abajo y utilizando todos los dedos.
2. En Estados Unidos éste es el símbolo de la paz pero en Europa significa "victoria". En algunos lugares de Europa, como el Reino Unido, hacer este gesto con la palma girada hacia dentro significa "¡que te den!".
3. En Estados Unidos, esto es simplemente una postura cómoda para sentarse y no tiene ninguna connotación negativa. Sin embargo, en otros países como Tailandia, Japón o Francia, así como en países de Oriente Próximo y Medio, mostrar las plantas de los pies es una falta de respeto. Exponer la parte más baja y más sucia del cuerpo resulta ofensivo.
4. En Estados Unidos, este gesto quiere decir que todo va bien. En otras partes del mundo tiene un significado totalmente distinto. En Brasil y Alemania es un gesto obsceno, en Japón significa "dinero" y en Francia se utiliza para indicar que algo no tiene ningún valor.
5. En Estados Unidos, al igual que en otros muchos países, este gesto se utiliza para saludar, es una forma de decir hola o adiós. Pero en algunos lugares de Europa puede significar "no" y en Nigeria es un insulto grave.
6. En muchos países mover la cabeza de esta forma es un modo de decir "sí", pero en lugares como Bulgaria o Grecia sirve para decir "no".

Éstos son sólo algunos ejemplos de gestos que pueden tener distintos significados, dependiendo del lugar en el que se encuentre o las personas con las que esté hablando. Es importante comprender los distintos significados de los gestos porque la comunicación casi siempre es mucho más que lo que se dice.

Esta sección pretende mostrar que, cuando se interactúa con un objetivo, estos principios no sólo deben tenerse en cuenta, sino que pueden utilizarse para manipular al objetivo. Por otro lado, conocer el origen cultural de sus objetivos evitará que realice gestos con significados indeseables.

El anclaje

Los gestos pueden tener efectos poderosos cuando se utilizan adecuadamente. Algunos de estos métodos provienen del estudio de la PNL y pueden ser muy efectivos a la hora de situar la mente del objetivo en cierta dirección.

Uno de esos métodos es el "anclaje", que consiste en conectar afirmaciones de parecido contenido con un gesto determinado. Por ejemplo, si está hablando con un objetivo y éste describe algo como bueno y positivo, puede repetir lo que él ha dicho haciendo un gesto con la mano derecha. Si menciona algo negativo, realiza un gesto con la mano izquierda. Después de repetir el proceso varias veces, en la mente del objetivo se crea este "anclaje" que le indica que los gestos con la mano derecha están relacionados con las cosas buenas.

Los vendedores utilizan este método para consolidar en sus objetivos una opinión positiva sobre su producto y una negativa sobre el producto de la competencia. Algunos políticos también se sirven de esta técnica para anclar pensamientos positivos o pensamientos que quieren que resulten positivos en su audiencia. Bill Clinton es un claro ejemplo de esto. Para ver este método en acción (aunque no al ex presidente Clinton) visite `www.youtube.com/watch?v=c1v4n3LKDto&feature=placer_embedded`.

El reflejo

Otra táctica gestual es el "reflejo", que consiste en hacer coincidir sus gestos con la personalidad del objetivo. Por supuesto, no es tan sencillo como parece pero, ¿qué puede deducir observando al objetivo? ¿Es tímido? ¿Es enérgico y extrovertido? Si aborda a una persona tímida con gestos agresivos es muy probable que la asuste y no pueda obtener lo que desea de ella.Del mismo modo, si usted es una persona tímida tendrá que imitar los gestos agresivos de la gente enérgica. El reflejo no consiste tan sólo en imitar el lenguaje corporal del objetivo, sino también en emplear gestos que faciliten que el objetivo le escuche.

Puede llevar este concepto a otro nivel. Para un objetivo puede ser muy reconfortante observar gestos con los que se siente familiarizado. No obstante, debe buscar un punto de equilibrio porque, si el objetivo utiliza muy a menudo un gesto concreto y decide imitarlo y emplear el gesto del mismo modo, corre el riesgo de que el objetivo se moleste. Debe imitarlo, pero no con exactitud. Si observa que al

terminar de exponer un pensamiento el objetivo coloca las manos en su barbilla, puede imitarlo colocando la mano en otra parte de su cara o dando un par de golpes en la barbilla con un dedo, después de exponer una idea.

La siguiente sección continúa analizando la gesticulación explicando la importancia de la posición de las manos y los brazos.

La posición de los brazos y las manos

Los agentes de la ley están entrenados para observar la posición y colocación de los brazos y las manos de los sospechosos durante los interrogatorios. Un aumento en los movimientos nerviosos durante un interrogatorio puede suponer un incremento de los niveles de estrés, que indicaría que el interrogatorio está teniendo el efecto deseado. Esto sería, por supuesto, en el caso de un interrogatorio policial; en una situación de ingeniería social deben observarse esos mismos signos, pero los signos de estrés pueden indicar que debe disminuir la presión (a no ser que la meta sea precisamente estresar al objetivo).

Los agentes del orden aprenden a prestar atención a dos signos en particular:

- Los codos normalmente cuelgan a los lados del cuerpo cuando una persona está relajada. Cuando se siente amenazada o atemorizada la reacción natural del cuerpo es juntar los codos contra las costillas. Básicamente, ésta es una postura instintiva de protección de los órganos internos que podrían verse amenazados.
- Los gestos de las manos también pueden ser muy reveladores. Un objetivo puede estar indicando con sus manos algo distinto a lo que está diciendo. Por ejemplo, en el interrogatorio de un sospechoso de un delito, éste puede estar haciendo gestos con las manos que describen una acción (como estrangular, disparar, apuñalar, etc.) pero sólo pronunciar la palabra crimen o incidente. Es muy importante observar los gestos sutiles que su objetivo puede hacer con las manos.

Si es capaz de detectar signos en su objetivo de que se siente amenazado o atemorizado podrá corregir la situación y hacer que vuelva a sentirse cómodo y tranquilo. Cuando aborda a un objetivo el lenguaje corporal y los gestos de las manos y los brazos pueden decirle muchas cosas, incluso antes de pronunciar la primera palabra. Otros gestos a los que debe prestarse atención son:

- Las palmas de las manos abiertas pueden indicar sinceridad.
- Los dedos de las dos manos unidos formando una "V" invertida, pueden significar que la persona posee cierto sentido de autoridad.

- Dar golpecitos en la mesa con los dedos suele ser una señal de tener problemas de ansiedad.
- Tocarse el rostro indica reflexión; tocarse el cabello puede ser un signo de inseguridad; tocarse las orejas es señal de indecisión.

Registrar estos gestos puede darle mucha información sobre la mentalidad de sus objetivos. Por otra parte, realizarlos le ayudará a representar fielmente un pretexto. A continuación, se enumeran algunos puntos clave sobre la gesticulación que es importante recordar, sobre todo si acostumbra a gesticular mucho, como es mi caso:

- La gente no debe recordar el gesto, sólo el mensaje unido a él. Si la gente comenta: "Vaya, este tipo gesticula muchísimo", debe considerar tomárselo con un poco más de calma. Lo importante es el mensaje, no el gesto.
- Evite la monotonía. Incluso gesticulando se puede ser tan soso, aburrido y repetitivo que el gesto acabe provocando que el objetivo tenga una percepción negativa de su interlocutor.
- Asegúrese de no mostrar signos de ansiedad, tales como dar golpecitos con los dedos o hacer movimientos bruscos y entrecortados. Le indican al objetivo que está nervioso y resulta contraproducente para el mensaje que quiere dar.
- El exceso es malo. Gesticular demasiado también va en contra del mensaje que pretende transmitir.

Recuerde que las expresiones faciales, la gesticulación y la postura va todo en el mismo paquete. Deben coordinarse, equilibrarse y emplearse para apoyar su pretexto.

A pesar de lo buena que pueda ser esta información, hay una herramienta fundamental para realizar interrogatorios exitosos.

Saber escuchar

Probablemente, no existe una habilidad más completa que ésta. Gran parte de la ingeniería social consiste en saber escuchar. Pero debe tener en cuenta que no es lo mismo "oír" que "escuchar".

Se cree que la gente retiene alrededor del 50 por 100 de lo que oye. Esto significa que, si habla con una persona durante diez minutos, sólo recordará unos cinco minutos de lo que le ha dicho. Aunque la mayoría de la gente se las arregla de esta manera, no es una situación aceptable para un ingeniero social.

A menudo, las cosas aparentemente más insignificantes son fundamentales para tener éxito. Por este motivo, es muy importante que mejore su capacidad de escucha, no sólo de lo que se dice, sino de cómo se dice, cuándo se dice y con qué emociones en juego. Todos estos factores contribuyen a formar su percepción sobre la información transmitida.

Ser bueno escuchando a los demás puede parecer fácil pero, cuando está en mitad de la acción tratando de acceder al cuarto de servidores y escuchando la conversación de unos empleados en un descanso, a los que pretende seguir para entrar al edificio, escuchar de verdad puede resultar muy difícil.

No obstante, es en esos momentos cuando resulta más importante escuchar con atención. Puede que Susan empiece a quejarse de su jefe de recursos humanos, el señor Jones. Explica lo brusco que ha sido con ella últimamente y lo harta que está de él. Entonces su compañera dice: "Bueno, entonces deberías pasarte por el maravilloso mundo de la contabilidad. Ahí sí que tenemos a unos cuantos idiotas".

Esto puede sonar como la típica conversación de dos empleadas cansadas y enfadadas. ¿O es algo más? Ahora tiene sus nombres, el nombre de un jefe, el nombre de sus departamentos y una idea sobre el comportamiento general de algunos de los empleados. Esta información puede ser muy útil más adelante cuando tenga explicar por qué se encuentra dentro del edificio.

A menudo, la forma que tiene alguien de decir las cosas puede revelar mucho sobre cómo es esa persona, pero para saber aplicar esta idea necesita escuchar bien. ¿Esa persona está triste, enfadada o contenta? ¿Reacciona con rapidez o con lentitud? ¿Es emocional o controla sus sentimientos? Muchas veces prestar atención a este tipo de detalles le puede decir más que las palabras.

Por lo tanto, ¿cómo lograr ser bueno escuchando a los demás?

Los siguientes pasos pueden ayudarle a perfeccionar su habilidad para escuchar a la gente. Estos consejos se pueden aplicar en el plano profesional y en el personal pero cuando se emplean en una auditoría de seguridad realmente marcan la diferencia.

1. **Preste atención:** Preste a su objetivo la máxima atención posible. No jugueteé con su teléfono móvil o con cualquier otra cosa. No dé golpecitos con los dedos. Intente centrarse en lo que se está diciendo y mire a la persona que habla. Hágalo con curiosidad, no de una forma amenazante o acosadora.

   Intente no adelantarse pensando en su próxima respuesta. Si está planeando su siguiente respuesta o refutación, significa que no está concentrado en lo que se está diciendo y puede perderse algo importante o darle al objetivo la impresión de que no le interesa lo que le cuenta. Esto puede ser muy difícil de controlar, para la mayoría de la gente perfeccionar esta idea cuesta mucho trabajo.

Procure no distraerse con factores externos. El ruido de fondo o un grupo de personas riéndose muy cerca puede descentrarle; no permita que esto ocurra.

Por último, preste mucha atención también a lo que el objetivo "no" está diciendo. Debe "escuchar" atentamente el lenguaje corporal, las expresiones faciales y otros aspectos de la comunicación.

2. **Demuestre que está escuchando:** Muéstrese abierto y receptivo con su lenguaje corporal y sus expresiones faciales. No de vez en cuando, ni tampoco demasiado a menudo, pero lo suficiente como para que el objetivo sepa que está con él. No debe parecer un robot que asiente a todo lo que dice, pero el objetivo debe notar su presencia.

   No olvide la importancia de la sonrisa. Sonriendo le dice al objetivo que está con él y que entiende lo que le dice. Igual que en el caso de la atención, sonría de vez en cuando, cuando lo considere adecuado. Si la persona le está contando que su perro acaba de morir, no tiene ningún sentido asentir y sonreír.

3. **Retroalimente a su interlocutor:** Es muy normal permitir que las creencias y experiencias propias filtren el mensaje que le están transmitiendo. Si lo hace, puede que no esté escuchando realmente el mensaje.

   Asegúrese de hacer preguntas relevantes. Si el objetivo le está hablando del cielo azul y usted pregunta: "Entonces, ¿era muy azul el cielo?", resultará evidente que no prestaba atención. Sus preguntas deben mostrar que ha estado escuchando y que está interesado en saber más sobre el asunto.

   Repetir o resumir lo que ha escuchado es una táctica que funciona si se aplica de vez en cuando. No recite la conversación como si la hubiera aprendido de memoria, recapitule algunos de los argumentos expuestos y le transmitirá al objetivo que sintoniza con su mensaje.

4. **No interrumpa:** No es necesario explicar mucho sobre este consejo. Interrumpir al objetivo muestra falta de interés por sus sentimientos y puede detener la interacción. Es mejor que le deje terminar y hable después.

   Sin embargo, hay ocasiones en que interrumpir puede ser útil a nivel táctico. Si quiere un ejemplo, vea la película *Los fisgones* (*Sneakers*). Cuando Robert Redford tiene que cruzar una puerta que está cerrada con llave, interrumpe la encendida discusión que mantiene el portero con otra persona. Lo hace varias veces hasta que finalmente el portero se siente frustrado y abre la puerta sin autorización. Si considera que puede sacar provecho puede ser buena idea interrumpir. Pero en la mayoría de ocasiones no lo es.

5. **Responda adecuadamente:** Éste es el punto cumbre de las habilidades para escuchar bien. Si está pensando en su contestación o en la rubia atractiva que acaba de pasar, meterá la pata.

En cierta ocasión, estaba impartiendo un curso y explicaba a un grupo de personas determinados aspectos de unas tácticas de manipulación muy detalladas. Me di cuenta de que había dos tipos que no estaban escuchando. Entonces dije una frase sin sentido: "Después horneas el león a 180 grados durante 15 minutos hasta que esté crujiente". El resto del grupo rompió a reír. Me dirigí a uno de los dos y dije: "¿Tú que piensas, John?". Me miró con cara inexpresiva y tartamudeó: "Emm, sí, suena muy bien".

Nunca le haga eso a un objetivo. Sería un golpe mortal a la compenetración (explicada más adelante en este capítulo) que pretende crear. Sea respetuoso, controle sus emociones y responda adecuadamente en todo momento cuando converse con su objetivo.

Por lo tanto, los puntos más importantes para escuchar bien son prestar atención, demostrar que está escuchando, proporcionar una retroalimentación positiva, tener cuidado para no interrumpir y responder adecuadamente. Todos ellos entran en juego especialmente en acciones de ingeniería social importantes, como cuando tuve que interactuar con el caballero de la reunión de la Cámara de Comercio con el que me "encontré" en la barra para hablar de negocios. Gran parte de la información que andaba buscando se reveló en una conversación normal y corriente. Asegúrese de practicar estos consejos en casa o en el trabajo antes de iniciar la conversación en cuestión. Es importante que saber escuchar bien sea una parte natural de sus armas, no algo en lo que debe estar pensando continuamente.

Otro aspecto que debe tomar en consideración para escuchar bien son sus propias emociones. Por ejemplo, yo me crié en una familia italiana muy religiosa y estricta. Me enseñaron que nunca se le falta el respeto a una mujer y tiemblo sólo con pensar en contar una ocasión en la que me dirigí a mi madre con un tono despectivo. Sólo diré que el asunto no acabó muy bien para mí. Muchas años después de ese incidente, estaba trabajando en una auditoría y estaba hablando con un hombre del que debía obtener cierta información. Me dirigí a él e iniciamos una conversación. Comenzó a hablar de una mujer con la que trabajaba de un modo muy inadecuado. Debido al modo en que fui educado, empecé a notar que la ira me quemaba por dentro. Me costó mucho trabajo contener esos sentimientos y mi rostro y mi lenguaje corporal debieron mostrarlos, estropeando aquella ocasión. Con aquel fracaso aprendí una lección valiosa. Cuando tenga que concentrarse en escuchar en una acción profesional, debe hacer todo lo posible porque las opiniones personales no se interpongan en el camino.

Además, recuerde que debe reaccionar al mensaje, no a la persona. Aunque no esté de acuerdo con las opiniones o creencias de una persona, si le permite expresarlas conseguirá que se sienta cómoda con usted. Incluso en situaciones de este tipo puede encontrar algo empático que decir. Por ejemplo:

Objetivo: "Este trabajo es una basura. Tengo que hacer este turno horrible y encima pagan poquísimo".

Ingeniero social: "Parece que está harto de su situación".

Aunque al ver esta respuesta puede pensar que se podría hacer mejor, contestando de esta forma está haciendo ver al objetivo que le está escuchando a la vez que empatiza con su difícil situación.

Esta técnica se conoce como "respuesta reflexiva". Sus principios básicos son los siguientes:

- Escuche activamente, como se ha explicado.
- Cuando llegue el momento de responder, preste atención a sus emociones. Identificar sus sentimientos mientras el objetivo habla le puede ayudar a reaccionar adecuadamente.
- Repita todo el contenido pero no como un loro, sino utilizando sus propias palabras.
- Comience su respuesta con una frase neutral como "parece que", "da la sensación" o "se diría que". Estas frases facilitan el mensaje que tiene que dar. Para comprobarlo, la próxima vez que discuta con una amigo, el jefe o sus padres, diga: "Estás enfadado conmigo porque..." y compare la reacción de esa persona con la que tiene si le dice: "Da la sensación de que estás enfadado porque...". Confirmará qué respuesta acepta mejor.

La respuesta reflexiva unida a saber escuchar de manera activa tiene mucha utilidad a la hora de construir confianza y compenetración.

Cuando le resulte natural escuchar mejor, mejorará su habilidad para reaccionar al mensaje transmitido. La meta del ingeniero social es reunir información, acceder a algún lugar o conseguir algo a lo que no debería tener acceso o lograr que el objetivo lleve a cabo una acción. Al pensar que deben dominar las técnicas de manipulación, muchas personas se olvidan de aprender a escuchar bien a los demás, pero precisamente ésa es la razón por la que debe ser bueno escuchando.

Considere estas dos situaciones:

- Un vecino le pide que le ayude en su garaje con un asunto durante una hora. Ese vecino tiene un perro que ha hurgado en su basura varias veces y que parece que tiene cierta tendencia a utilizar su jardín como cuarto de

baño. Además, cuando el vecino viene a pedirle el favor, estaba a punto de sentarse a relajarse viendo la televisión o leyendo un libro después de un largo día de trabajo.

- Un amigo de la infancia viene a pedirle ayuda para mover unos muebles. Acaba de mudarse a un apartamento a cinco kilómetros de distancia y no consigue subir el sofá por las escaleras. Cuando llega estaba a punto de sentarse a descansar.

¿En qué situación estará más dispuesto ayudar? La mayoría de la gente estaría más dispuesta en la segunda situación. En el primer caso, pondrían una excusa para no ayudar o para aplazarlo a otro momento más conveniente.

¿Por qué? La gente es muy abierta con sus amigos. Cuando se siente a gusto con alguien, no pone barreras y puede dejar de lado sus propios deseos para ayudarle en un momento dado. Además, de forma natural se confía en el mensaje que proviene de un amigo, mientras que con un desconocido se tiende a buscar segundas intenciones y a dudar de la sinceridad de la propuesta. En el caso de la relación con un amigo, esa conexión existente se llama "compenetración".

Durante años sólo se ha hablado de la compenetración en el campo de las ventas o las negociaciones. La compenetración no es sólo para vendedores; es una herramienta que cualquiera puede utilizar, en especial los ingenieros sociales. La siguiente sección explica cómo generar compenetración al instante.

Crear compenetración instantánea

Mi ex compañero de trabajo, Tony, solía decir que crear compenetración es más importante que respirar. No creo que esto sea cierto, pero sí es verdad que es una idea fundamental.

La Wikipedia define la compenetración como "uno de los aspectos o características más importantes de la interacción humana inconsciente. Consiste en tener una perspectiva común: estar 'en sintonía' o 'en la misma onda' con la persona que se está hablando".

¿Por qué explicamos la compenetración en este capítulo? Porque es un elemento clave para desarrollar una relación con otra persona. Sin compenetración está en un punto muerto. Ente los principios psicológicos de la ingeniería social, la compenetración es uno de los pilares. Antes de aprender a utilizar la compenetración, debe comprender cómo crearla.

Imagine que pudiera hacer que la gente que conoce quisiera hablarle, contarle la historia de su vida y estuviera predispuesta a confiar en usted. ¿Alguna vez ha conocido a alguien así? ¿Alguien a quien nada más conocer se ha sentido cómodo

contándole asuntos muy personales? Puede haber muchas razones psicológicas para que esto suceda, pero es probable que el motivo sea que se ha generado compenetración.

En la siguiente sección, explicamos algunos puntos importantes para crear compenetración y cómo utilizarla.

Sea sincero en su deseo de conocer a la gente

¿Hasta qué punto la gente es importante para usted? ¿Le gusta conocer gente nueva? Esto es una mentalidad ante la vida, no es algo que se pueda aprender. El requisito previo para crear compenetración es que le guste la gente. La gente se da cuenta cuando hay intereses falsos.

Para ser un buen ingeniero social y ser capaz de utilizar la compenetración, tiene que dar importancia a las personas. Debe gustarle la gente y disfrutar interactuando con ella. Debe desear aprender de las personas. La gente percibe las sonrisas falsas y las dobles intenciones. Para crear compenetración es necesario desarrollar un interés sincero por su objetivo.

Cuide su aspecto

Algunas cosas que pueden afectar a su interacción con los demás no se pueden cambiar. Desgraciadamente, es inevitable que algunas personas le juzguen por el color de su piel, su género o su edad, antes de interactuar con ellas. Son cosas que no se pueden controlar, pero hay otros aspectos que sí pueden controlarse, como la vestimenta, el olor corporal, la higiene, así como el contacto visual, los movimientos corporales y las expresiones faciales. En cierta ocasión, leí una afirmación que el tiempo me ha demostrado que es totalmente cierta: "Si una persona no se siente a gusto consigo misma, los demás tampoco se sentirán a gusto con ella".

Tenga en cuenta su pretexto y a su objetivo. Si su pretexto es ser el conserje, asegúrese de comportarse, vestirse y hablar como uno. Si su pretexto es ser el gerente de un negocio, actúe y vístase de forma adecuada. Necesitará investigar al respecto pero nada es más devastador para la compenetración que no tener el aspecto apropiado. Su meta en ciertas situaciones es lograr que la gente actúe con el piloto automático y no le cuestione. Si su vestimenta, su aspecto o su conducta no son adecuados, el objetivo deja el piloto automático y se evaporan sus opciones de tener éxito.

Aprenda a escuchar a las personas

Consulte la sección anterior sobre este tema. Saber escuchar tiene una importancia vital.

Tanto si está haciendo amigos como si está realizando una acción de ingeniería social, debe dominar el arte de escuchar a la gente.

Sea consciente de cómo afecta a las personas

En cierta ocasión, vi cómo se le caía algo a una señora muy mayor mientras salía de una tienda. Recogí lo que se le había caído y la seguí al aparcamiento. Cuando la alcancé ya estaba metiendo las bolsas de la compra en el maletero. Aparecí por detrás de esta pequeña señora y con mi 1,90, casi abalanzándome sobre ella, dije: "Perdone, señora". Obviamente, me acerqué más de la cuenta y la anciana se dio la vuelta y empezó a gritar: "¡Socorro, me quieren atracar! ¡Socorro!".

Tenía que haber pensado cómo podría afectar mi presencia a esta mujer. Era probable que una señora mayor sola en un aparcamiento, que no esperaba que un hombre grande se le acercara, se pusiera nerviosa. Tenía que haber dado la vuelta y haberme acercado desde otro ángulo.

Piense cómo puede afectar su presencia y otros aspectos personales a las personas con las que entra en contacto. ¿Quizá necesita un chicle para el aliento? Asegúrese de que no tiene restos de comida en la cara o en los dientes. Intente que no haya nada en su aspecto que pueda alejar a la persona.

El profesor de psicología de la UCLA (Universidad de Los Ángeles, California), Albert Mehrabian, es célebre por la regla 7-38-55, que afirma que las estadísticas muestran que sólo el 7 por 100 de una comunicación normal está en las palabras que decimos, mientras que el resto de la comunicación reside en el lenguaje corporal y los tonos de voz.

Intente ser consciente de sí mismo, pero también preste atención a los primeros segundos de interacción con otra persona. Su primera reacción puede indicarle si ha olvidado algún detalle o si debe realizar algún cambio para ser más efectivo.

Debe ser consciente de cómo afecta a la gente. Si lo único en lo que piensa es en su meta final, afectará negativamente a las personas con las que entre en contacto. Piense en cómo afectarán su aspecto, sus palabras y su lenguaje corporal a sus objetivos. Debe resultar abierto y predispuesto.

Evite que la conversación se centre en usted

A todos nos encanta hablar de nosotros mismos, sobre todo si creemos que tenemos una historia genial para compartir; está en la naturaleza humana. Pero hablar de uno mismo es una forma de eliminar la compenetración. Deje que la otra persona hable de sí misma hasta que se canse; si lo hace, le considerarán un "gran amigo", un "marido perfecto", una persona que "realmente sabe escuchar", un "vendedor perfecto" o cualquier otra etiqueta que esté buscando. La gente se siente bien cuando puede hablar de sí misma; supongo que todos somos un poco narcisistas, pero si deja que sea la otra persona la que hable, conseguirá gustarle mucho más.

Evite que la conversación se centre en usted. Este argumento es especialmente aplicable a un ingeniero social. Al tener una meta bien definida en mente, puede suceder que su juicio y dirección se enturbien por lo que persigue. La conversación debe girar alrededor del objetivo para que sea exitosa. Deje que hable de su trabajo y sus proyectos y le sorprenderá la cantidad de información que revela.

Recuerde que la empatía es la clave de la compenetración

La empatía, definida en el *Random House Dictionary* como "la identificación intelectual con o la vivencia indirecta de las emociones, pensamientos o actitudes de otro", es una característica de la que carece mucha gente hoy en día y es especialmente difícil de sentir si considera que tiene la solución a los problemas de otro. No obstante, si escucha de verdad lo que alguien le cuenta, intentando identificarse y comprender las emociones subyacentes, y utiliza después sus habilidades para proyectar esos sentimientos, conseguirá que la persona sienta que está en auténtica sintonía con él.

He considerado necesario aportar la definición de empatía porque es importante entender lo que debe hacer. Observe que es necesario "identificarse intelectualmente" con y experimentar "las emociones, pensamientos o actitudes" de otra persona.

Estas emociones no siempre son serias, deprimentes o radicales. Puede ser útil incluso entender por qué alguien está tenso, cansado o de mal humor. Imagine que va al banco y la cajera se enfada con usted porque ha olvidado firmar el cheque y ahora lo tiene que enviar de vuelta. Además, ha olvidado traer un bolígrafo y tiene que pedirle otro favor más. Su reacción posiblemente sería parecida a la mía, sobre todo si le lanza la mirada de enfado: le gustaría decirle que ella está ahí para

servirle. En cambio, pruebe a decir: "Parece que está un poco molesta, lo entiendo; a mí también me molesta cuando trato con mis clientes olvidadizos. Siento tener que pedírselo pero ¿podría dejarme un bolígrafo?".

Es importante no resultar condescendiente cuando muestre empatía. Si se muestra altivo o arrogante, el objetivo tendrá la sensación de que está siendo condescendiente.

En el ejemplo anterior, reconoce que la cajera está molesta pero sin acusarla, le indica que usted tiene el mismo tipo de sentimientos y después hace su petición. La empatía puede ser muy útil para crear compenetración; hay que advertir que la compenetración no se puede fingir. La gente debe sentir que está realmente interesado en crear esa relación de confianza. Si le cuesta mostrar empatía de forma natural, practique con su familia, amigos, compañeros de trabajo y profesores. De esta forma, mejorará enormemente su habilidad para crear relaciones personales.

La empatía es una herramienta importante del ingeniero social. Desgraciadamente, también se utiliza muy a menudo con malas intenciones. Cuando sucede una catástrofe en alguna parte del mundo, aparece enseguida un ingeniero social malicioso para "empatizar". Probablemente les resulte tan fácil utilizar esta herramienta porque ellos mismos han vivido situaciones difíciles y vienen de entornos complicados. Al haber pasado apuros, consiguen fácilmente resultar empáticos con las dificultades de los demás, por lo que se crea una compenetración rápidamente.

Nada genera más compenetración que la sensación de que la otra persona le "entiende". Esto se demuestra cuando alguien es víctima de una desgracia. Es una idea algo inquietante, pero quienes han sido víctimas de abusos, crímenes, violaciones, desastres naturales, guerras u otras atrocidades, normalmente pueden "entender" los sentimientos de otras personas que sufren situaciones parecidas. Esto puede hacer que una víctima confíe en la persona equivocada si se ha creado compenetración.

Como mencionamos anteriormente, a raíz de los ataques del 11 de septiembre en Nueva York, muchas personas afirmaron haber perdido familiares y amigos en ataques terroristas. Esto hizo que la gente sintiera empatía por estas "víctimas", que obtuvieron dinero, fama o lo que estuvieran buscando.

Como auditor de seguridad debe contar con una amplia gama de sentimientos que utilizar. Si se cierra a sus emociones es muy difícil generar empatía. Este punto está relacionado con apreciar realmente a las personas. Si lo hace, no le costará mucho trabajo comprenderlas y empatizar con ellas.

Tenga una cultura general amplia

El conocimiento es poder. No tiene que saberlo todo de todos los temas pero conviene tener conocimientos sobre ciertos asuntos. Hace que resulte interesante y le da una base sobre la que iniciar conversaciones.

El conocimiento es poder. El viejo lema hacker tiene un gran valor en ingeniería social. Un auditor de seguridad debe ser buen lector y estudioso. Si su cultura es amplia tendrá algo de lo que hablar cuando aborde a un objetivo. No deje de leer, investigar y estudiar sobre los temas a los que se dedica el objetivo en su trabajo o en su tiempo libre. La meta no es convertirse en un "sabelotodo" experto en cualquier materia, sino tener el conocimiento suficiente para no mirar al objetivo desconcertado cuando éste le pregunte: "¿Has traído un conector RJ-45 para solucionar los problemas de conexión de red del servidor?".

Desarrolle su curiosidad

A menudo, la gente se muestra demasiado segura de sí misma en lo que se refiere a sus ideas de cómo se deben hacer las cosas. Esa actitud rígida puede cambiar la forma en que se reacciona ante las cosas que se dicen. Incluso sin decir nada, puede empezar a pensarlo y mostrarlo en su lenguaje corporal o sus expresiones faciales. En lugar de mantenerse rígido en sus creencias, sea curioso respecto a lo que los demás piensan y al modo en que hacen las cosas. De esta forma, evitará hacer juicios precipitados. Puede aplicar esta idea siendo lo suficientemente humilde como para pedir ayuda o más información sobre cierto asunto a alguien. Sea abierto de mente para aceptar las opiniones de los demás, aunque éstas sean diferentes a las suyas.

Cuando siente curiosidad por otros estilos de vida, culturas y lenguas, empieza a comprender lo que motiva a la gente. También evita que sea rígido e inflexible en sus opiniones. Puede que no esté de acuerdo con ciertas opiniones y creencias pero, si se mantiene abierto y no emite juicios de valor, podrá interactuar con alguien comprendiendo por qué reacciona y se comporta de cierta manera, en lugar de juzgarlo.

Encuentre el modo de satisfacer las necesidades de los demás

Éste es el punto culmen de la lista y uno de los más importantes del libro. El doctor William Glasser escribió un libro llamado *Teoría de la elección: una nueva psicología de la libertad personal* en el que identificaba cuatro necesidades psicológicas fundamentales para el ser humano:

- Pertenencia/conexión/amor.
- Poder/relevancia/capacidad.
- Libertad/responsabilidad.
- Diversión/aprendizaje.

El argumento clave que esconde este punto es que, logrando que la gente satisfaga estas necesidades conversando con usted, conseguirá una compenetración inmediata. Si crea un entorno para proporcionar estas necesidades a la gente, creará unos vínculos inquebrantables.

Permítame que le cuente una historia sobre la importancia de satisfacer las necesidades de los demás. Años atrás me vi involucrado en un accidente de coche. Un conductor joven salió delante de mí en la carretera y frenó de repente. En una fracción de segundo tenía que decidir si chocarme contra él a 90 kilómetros por hora o girar para lanzar mi coche hacia la cuneta a los pies de una montaña. Elegí la segunda opción para evitar matar a los tres jóvenes que viajaban en el otro coche. Salí volando hasta chocar contra la roca. Mi precioso Jetta "customizado" se destrozó con el choque y me golpeé la cabeza contra el parabrisas. Rocé ligeramente el parachoques del otro coche, que se quedó atravesado en mitad de la autopista. Cuando recuperé la orientación, llamamos a la ambulancia y a la policía.

El muchacho del otro coche tenía una aseguradora distinta a la mía. A la mañana siguiente recibí una llamada de su agente que me hizo una serie de preguntas. Me comentó que un perito pasaría a revisar mi coche y en 48 horas recibí un cheque y una carta afirmando que correrían con los gastos médicos de mi recuperación.

Más adelante, recibí una llamada de "su" agente de seguros para interesarse por mi estado. ¿Cuántas llamadas de mi compañía de seguros recibí? Sólo una para explicarme cómo debía contestar a las preguntas que me hicieran.

Comprendí que en estas grandes compañías preocuparse por las personas no es una prioridad. Sin embargo, el otro agente me había llamado simplemente para comprobar si me encontraba bien. No tuve ningún problema para que me pagaran y me dieron un precio justo por mi coche.

Dos días después, cancelé mi seguro y fui a ver a Eric, el agente de seguros del joven del accidente. Le dije que me había gustado tanto el trato recibido que quería contratar sus servicios. Han pasado 12 años y Eric sigue siendo mi agente para cualquier seguro que contrato. Hace dos años recibí una llamada de una aseguradora que me ofrecía unas tarifas considerablemente más bajas que las de Eric, pero ni siquiera se me pasó por la cabeza cambiar de compañía y dejar a Eric en la estacada. ¿Por qué? Compenetración, pura y simple. Eric es mi amigo, mi ayudante, alguien a quien puedo llamar para cualquier asunto relacionado con seguros y que siempre me da el mejor consejo posible. Conoce a mi familia, se preocupa por nosotros y nunca insiste para convencerme. Tampoco tiene por qué hacerlo porque confío en él y siempre compro lo que me ofrece. Ése es el poder de la compenetración. Quizá lo que pretendía Eric cuando llamó para comprobar qué tal estaba era que acabara contratándole, no lo sé, aunque lo dudo. Conociéndole,

sé que se preocupa por los demás y cualquiera que le conozca dice lo mismo. Su hermano y él dirigen un buen negocio. La compenetración puede crear vínculos entre la gente que trascienden los costes o las pérdidas.

Si cubre una necesidad de la persona con la que habla, las opciones de crear compenetración aumentan drásticamente. Hágalo sin que parezca que tiene segundas intenciones, hágalo con el deseo auténtico de ayudar y se sorprenderá con los resultados. Probablemente, no hay herramienta más valiosa para un ingeniero social que la de ser capaz de satisfacer estas necesidades de las personas. Si aprende a crear entornos favorables en los que el objetivo puede cubrir alguna de estas cuatro necesidades básicas, logrará una compenetración inquebrantable.

Los espías utilizan a menudo este método de satisfacer necesidades o deseos. En un viaje reciente a un país latinoamericano, me comentaron que su gobierno sufre infiltraciones constantes con la táctica de satisfacer la necesidad de "conexión o amor". Envían a una mujer hermosa para que seduzca a un hombre, pero no por una noche. Lo seduce durante días, semanas, meses o incluso años. Según va pasando el tiempo, sus peticiones se van haciendo más atrevidas y más personales, consiguiendo finalmente acceder a su despacho, donde instala micrófonos, troyanos o unidades clonadas. Este método es devastador y funciona.

Otra técnica que se emplea frecuentemente para "satisfacer" deseos es el *phishing*. En un test se enviaron a 125 empleados de una compañía importante unos archivos de imagen falsos con nombres como `BritneyDesnuda.jpg`, `MileyCyrusDuchandose.jpg` y otros nombres por el estilo. Cada imagen contenía código malicioso que daba al ingeniero social acceso al ordenador del usuario. El resultado fue que se abrieron más del 75 por 100 de las imágenes. Se descubrió que, cuanto más joven era la chica mencionada en el nombre del archivo, mayor era la proporción de descargas.

Estos hechos vergonzosos muestran lo bien que funciona la idea de satisfacer los deseos de las personas. En persona, los resultados son parecidos. Los interrogadores policiales utilizan esta táctica continuamente para crear compenetración.

En cierta ocasión, entrevisté a un agente de la ley para un *podcast* que realicé en `social-engineer.org` (`www.social.engineer.org/framework/Podcast/001_-_Interrogation_and_Interview_Tactics`). Mi invitado contó una historia que demuestra el poder de la compenetración para lograr que la gente acceda a lo que se le pide. Los agentes habían arrestado a un *voyeur*. Era un fetichista al que le gustaba invadir la privacidad de mujeres que calzaban botas vaqueras de color rosa. Los agentes, en lugar de juzgarle por el bicho raro que era, le decían cosas como: "A mí las botas que me gustan son las de color rojo" y "El otro día vi a una chica en minifalda y con botas vaqueras, ¡madre mía!".

Enseguida el sospechoso empezó a relajarse. ¿Por qué? Estaba rodeado de personas como él. Sintió que conectaba, que era uno más. Sus comentarios hicieron que se sintiera cómodo y empezó a sincerarse sobre sus "hábitos". Éste es un buen ejemplo sobre cómo desarrollar y crear compenetración, pero ¿cómo puede utilizarse en ingeniería social? Puede crear compenetración en cuestión de segundos aplicando los principios explicados anteriormente. Para comprobarlo, imagine que necesita dinero en efectivo pero no tiene su tarjeta de crédito y ha olvidado el número de cuenta, así que tiene que entrar y pedir ayuda. Quizá le dé cierta vergüenza tener que preguntar su número de cuenta. Entra en una sucursal de su banco en la que nunca ha estado antes. No hay nadie en el banco y puede elegir la ventanilla que prefiera. Puede que no se dé cuenta, la mayoría de la gente no lo hace, pero mira todas las ventanillas libres y elige al cajero que le hace sentir más cómodo. Obtendría los mismos resultados en cualquier ventanilla, pero elige la que le hace sentir mejor.

Quizá elige a la persona más atractiva o a la que muestra la sonrisa más amplia o a la primera que le saluda. Elija a quien elija y por el motivo que sea, sea una elección consciente o inconsciente, tiene mucho que ver con la compenetración. El mismo principio se aplica en su relación con un objetivo. En cuanto se acerque a él, empezará a hacer pequeños juicios en base a su apariencia, su conducta, sus expresiones faciales y, por supuesto, su estado de ánimo. Puede controlar muchos de estos factores, así que tome medidas al respecto y tendrá éxito en su actuación.

Desarrollar una buena compenetración crea un vínculo tan fuerte que puede mantenerse a pesar de algún inconveniente o malentendido sin importancia.

La compenetración permite a una persona decir y hacer cosas que sólo pueden hacer los buenos amigos, porque consigue que esa persona entre en el círculo de confianza. Es una fuerza poderosa sin la cual las amistades, las relaciones comerciales o laborales y muchas otras situaciones son bastante más complicadas. ¿Recuerda el concepto del pretexto, explicado en el capítulo 4? Aprendió que el pretexto es mucho más que interpretar un papel, es convertirse ante el objetivo en la persona que está retratando. Para lograr una buena compenetración es primordial desarrollar un pretexto sólido. En muchas de sus actuaciones profesionales no tendrá tiempo para idear un argumento ni para utilizar técnicas de compenetración a largo plazo, por lo que su éxito dependerá de muchas de las acciones no verbales que lleve a cabo.

Utilizar otras técnicas para crear compenetración

Existen otras técnicas para crear compenetración que se basan en la investigación de la PNL. La compenetración consiste básicamente en conectar con otro y hacer que se sienta cómodo; algunas técnicas utilizadas por hipnotizadores y profesionales de la PNL consiguen relajar a la gente al instante, como se explica a continuación.

Respirar al mismo ritmo que el objetivo

Respirar al mismo ritmo que otra persona no consiste en escuchar atentamente cómo respira y tratar de respirar cuando lo haga ella. Pero algunas personas tiene patrones de respiración muy definidos: hay quien tiene una respiración rápida y corta y hay quien tiene una respiración larga y profunda. Observe cómo respira su objetivo e imite ese patrón pero sin respirar exactamente igual y al mismo tiempo.

Igualar el tono de voz y la forma de hablar del objetivo

Yo nací en Nueva York y me crié en el seno de una familia italiana. Hablo rápido, alto y utilizando las manos. Además de ser en un 75 por 100 italiano, en el 25 por 100 restante soy húngaro. Soy grande, alto y gesticulo como si estuviera hablando por signos. Si abordo a un objetivo tranquilo y tímido que habla bajo y despacio, puedo arruinar compenetración si no calmo mi forma de hablar, procuro no gesticular y cambio mi estilo. Escuche el tono de voz de su objetivo e iguálelo, ya sea lento, rápido, alto, tranquilo o suave. Respecto a los acentos, la mejor regla es: no lo intente. A no ser que pueda imitar un acento realmente bien, no lo haga. Si la imitación es mala la compenetración será imposible.

En este sentido, también puede intentar retener algunas "muletillas". La gente utiliza términos como "es decir" o "¿vale?". Preste atención a las muletillas e intente introducirlas en alguna frase.

En cierta ocasión, estaba hablando con un objetivo que decía todo el tiempo: "Esto es tres cuartas partes de lo mismo". Yo no utilizo este tipo de expresión y no quería meter la pata, porque estropearía la compenetración. Lo que hice fue utilizar alguna palabra clave de esa expresión para decir cosas como "a mí me gusta ir por 'partes'".

La forma de hablar de las personas es otra área sobre la que es preferible no emitir juicios personales. Hay personas a las que les gusta acercarse para hablar, otras susurran y a otras les gusta tocar a su interlocutor. Debe permitir que el objetivo hable del modo en que se sienta más cómodo y después tratar de imitar su estilo.

Igualar el lenguaje corporal del objetivo

Ésta es un área muy interesante de la compenetración porque puede servir para crear vínculos fuertes pero también puede arruinar la compenetración si se hace mal.

Si observa que alguien tiene una postura determinada, con los brazos cruzados por ejemplo, no dé por sentado que le está rechazando, puede que tenga frío. Puede cruzar un brazo sobre su cuerpo para imitar su postura o entrelazar los dedos de las manos. Si está sentado frente a alguien que está comiendo, puede dar tragos de agua cuando come para imitarle. No haga exactamente lo mismo que él, realice acciones similares.

A la gente le gusta la gente que es como ella. Es la naturaleza humana. Les hace sentirse bien. Bill Philips es el genio que estaba detrás del programa *Body-for-Life*, que cambió el modo de hacer programas de entrenamiento físico. Promovía una idea que está muy relacionada con el principio de la imitación. Si es una persona con sobrepeso y siempre se relaciona con personas que también tienen sobrepeso, las probabilidades de que cambie son muy escasas. ¿Por qué? La respuesta es que estará a gusto con su sobrepeso y con la gente que también se encuentra bien de esa manera. Si quiere cambiar, relaciónese con gente delgada y enseguida experimentará un cambio de mentalidad.

Este principio se aplica de igual forma en ingeniería social. No quiere que su objetivo cambie, por lo que tiene que llegar a ser como él. Debe lograr que se sienta cómo con usted.

Probar la compenetración

Utilizar estas técnicas alternativas, así como igualar los niveles de energía o las expresiones faciales pueden generar una compenetración intensa en un plano subliminal. Después de practicar estas técnicas, puede ponerlas a prueba con un objetivo. Haga un movimiento como rascarse la cabeza o tocarse una oreja y si en los minutos siguientes su objetivo hace un movimiento similar, probablemente habrá conseguido compenetrarse con él.

Estas técnicas pueden ser de gran ayuda en sus relaciones con los demás. Aprenda a utilizar los principios psicológicos explicados en este capítulo y marcará la diferencia en su práctica profesional.

La siguiente sección revela la información más asombrosa de este libro.

El desbordamiento de búfer humano

Un vaso sólo puede contener cierta cantidad de líquido. Si tiene un vaso de 25 centilitros e intenta verter en él 35 centilitros de líquido, ¿qué sucede? El vaso se desbordará y el líquido se derramará por todas partes. Si intenta forzar el vaso para que contenga más líquido del que cabe en él, puede llegar a romperlo debido a la presión.

Los programas informáticos funcionan de un modo parecido. Imagine que tiene un pequeño programa que tiene un solo propósito y dos campos: Nombre de usuario y Contraseña.

Cuando se abre el programa aparece una pequeña pantalla en la que introduce **admin** en el campo Nombre de usuario y **contraseña** en el campo Contraseña. Aparece entonces un cuadro de diálogo en el que se puede leer "OK", lo que significa que todo está correcto.

El desarrollador del programa ha previsto cierta cantidad de espacio de memoria para el campo Nombre de usuario, el suficiente para que se pueda escribir la palabra "admin." dos veces. ¿Qué sucede si escribe veinte veces la letra A en ese campo y hace clic en **OK**?

El programa se colapsa y le da un mensaje de error. ¿Por qué? El dato introducido es más largo que el espacio asignado y sin la gestión de errores adecuada el programa emite una excepción y se colapsa.

La meta de los piratas informáticos es encontrar la dirección que el programa solicita en un colapso e insertar código malicioso en esa dirección. Al controlar el flujo de ejecución el hacker puede hacer que el programa "ejecute" las operaciones que desee. Puede introducir órdenes de todo tipo en el espacio de memoria del programa, porque tiene el control sobre él. Pocas cosas hay más emocionantes para un probador de seguridad que ver cómo un programa ejecuta las órdenes que le da.

La mente humana también ejecuta "software" y a lo largo de los años crea conjuntos de instrucciones, tamaños de búfer y espacios de memoria en su "paquete de software".

Antes de aplicar este concepto a la mente humana, es necesario definir algunos términos técnicos. Un "búfer" es un espacio que se reserva para que suceda algo o para almacenar datos.

En el ejemplo anterior, al campo Contraseña se le asigna un búfer, que es el número de caracteres que puede contener. En el caso de que se introduzca un número mayor del establecido, el programador debe indicarle al programa qué hacer con los datos sobrantes.

Si no lo hace, el programa se colapsa y el ordenador se apaga. Normalmente, lo que sucede es que el programa no sabe qué hacer con los datos sobrantes, por lo que desborda el espacio de almacenamiento, se colapsa y se cierra. De ahí proviene el término "desbordamiento de búfer".

La mente humana funciona de un modo parecido. Se reservan espacios para ciertos conjuntos de información. Si un conjunto de información no cabe en el espacio que tiene reservado, ¿qué sucede? El cerebro no se colapsa como un ordenador, pero se abre un hueco momentáneo que permite que se introduzca una orden que le diga al cerebro qué hacer con los datos sobrantes.

El desbordamiento de búfer humano aplica este principio. La meta es identificar un "programa" en ejecución e insertar código que le permita introducir órdenes para conducir el pensamiento en cierta dirección.

Para comprobar este concepto, observe este sencillo ejemplo que se muestra a continuación (véase la figura 5.15).



Figura 5.15. *Desbordamiento de búfer humano. Experimento 1.*

Debido a que las imágenes de este libro están en blanco y negro, he dejado una copia en color en el sitio Web en `www.social-engineer.org/resources/book/HumanBufferOverflow1.jpg`.

Éste es el ejercicio. Abra la URL y, lo más rápidamente que pueda, intente decir el color en que está escrita la palabra, no lo que dice la palabra.

Este juego es más difícil de lo que parece. Si consigue hacerlo, inténtelo cada vez más y más rápido. Lo que nos sucede a la mayoría de nosotros es que, al menos una vez, leemos la palabra en vez de decir el color o en algún momento nos cuesta hacerlo correctamente.

¿Por qué nos cuesta tanto realizar este ejercicio? Debido a las órdenes introducidas. Nuestro cerebro quiere leer la palabra, no el color, porque ésa es la forma en que funciona. Nuestro cerebro ve el color pero reacciona antes leyendo la palabra. Por lo tanto, el pensamiento en nuestra mente es la "palabra", no el color. Este ejercicio muestra que es posible ejecutar "código" en la mente humana contrario al pensamiento de la persona.

Establecer las reglas

En un artículo llamado "Modification of Audible and Visual Speech" (Modificación del habla audible y visual) que puede consultar en `www.prometheus-inc.com/asi/multimedia1998/papers/covell.pdf`, los investigadores Michele Covell, Malcolm Slaney, Cristoph Bregler y Margaret Withgott afirman que los científicos han demostrado que las personas hablan a una velo-

cidad de 150 palabras por minuto pero piensan a una velocidad de entre 500 y 600 palabras por minuto. Esto significa que la mayoría de las personas con las que habla pueden saltar de un lado a otro de la conversación en su mente. Por lo tanto, desbordar el cerebro hablando rápido parece casi imposible.

También debe comprender cómo la gente toma las decisiones en la vida. La mayoría de decisiones se toman de manera subconsciente. La gente conduce hasta el trabajo, prepara un café, se limpia los dientes y se viste sin pararse a pensar en ello en realidad.

¿Alguna vez ha conducido hasta el trabajo y después no recordaba los carteles que había por el camino o la ruta que ha seguido hasta allí? Cuando conducía estaba en un estado mental en el que el subconsciente estaba al mando y hacía lo que hace habitualmente sin pensar de manera consciente en cada paso.

La mayoría de las decisiones se toman de esta manera. Algunos científicos creen incluso que las decisiones se toman siete segundos antes en el subconsciente que en la vida real. Cuando la persona finalmente toma la decisión, lo hace en base a algo más que lo que escucha: la vista, los sentimientos y las emociones forman parte en la decisión.

Comprender cómo funcionan y piensan los seres humanos es la forma más rápida para provocar un desbordamiento de búfer o un desbordamiento de los programas naturales de la mente humana con el fin de introducir órdenes en ella.

Distorsionar el sistema operativo humano

En el mundo del pirateo informático, existe un método denominado "distorsión" que se utiliza para encontrar errores que puedan sobrescribirse para darle el control al hacker. La distorsión tiene lugar cuando el hacker introduce datos aleatorios de distinta extensión en el programa para comprobar cuándo colapsa por un exceso de datos. En ese momento, el hacker obtiene una vía para introducir código malicioso.

Del mismo modo, debe comprender cómo reacciona la mente humana a ciertos tipos de datos. Al plantear a una persona diferentes conjuntos de decisiones o diferentes conjuntos de datos y observar después cómo reaccionan, se puede descubrir los tipos de "programas" que están ejecutando. Existen ciertas leyes inherentes en la mente humana que todo el mundo cumple.

Por ejemplo, si se acerca a un edificio con puertas dobles (puertas externas e internas) y mantiene abierta la puerta externa para permitir el paso de un desconocido, ¿qué cree que hará esa persona después? Abrirá las puertas interiores para dejarle pasar.

Si está en medio de un atasco y permite que otro coche se incorpore delante de usted, lo más probable es que si más adelante usted necesita incorporarse, esa persona le permita hacerlo. ¿Por qué?

La razón tiene que ver con la "ley de las expectativas", que afirma que la gente normalmente cumple con lo que se espera de ella. Las decisiones se toman en base a las expectativas creadas. Un modo de empezar a enviar "información" maliciosa a la mente es la "presuposición".

Dándole algo primero al objetivo, puede después "esperar" que acceda a su petición. Una forma sencilla de comprobarlo es con el ejemplo de las puertas. Mantenga una puerta abierta para alguien y lo más probable es que esa persona procure abrir para usted la siguiente puerta. En una auditoría de seguridad, puede dedicarle un cumplido al objetivo o revelarle una información que pueda considerar valiosa antes de formular su petición. Procediendo de esta manera genera en el objetivo la necesidad de acceder a su petición, ya que es lo que se espera que haga.

La presuposición se puede explicar mejor con un ejemplo:

"¿Sabía que mi vecino, Ralph, siempre conduce un Ford Escort verde?"

En esta pregunta se presupone:

- Que conozco a mi vecino.
- Que se llama Ralph.
- Que tiene carné de conducir.
- Que conduce un coche verde.

Para emplear la presuposición de manera efectiva, debe formular la pregunta utilizando unas palabras, un lenguaje corporal y una expresión facial que indique que lo que pregunta se acepta de antemano. La clave de este método es evitar la "barrera" (la mente consciente) y acceder directamente a la "raíz del sistema" (el subconsciente). La forma más rápida de introducir su propio "código" es a través de órdenes incrustadas.

Las reglas de las órdenes incrustadas

Las órdenes incrustadas funcionan debido a ciertos principios fundamentales:

- Normalmente las órdenes son cortas: de tres o cuatro palabras.
- Para que sean efectivas necesitan que se ponga cierto énfasis en ellas.
- El mejor modo para que funcionen correctamente es escondiéndolas en frases normales.
- Su lenguaje corporal y facial debe ser acorde a las órdenes.

Las órdenes incrustadas son muy comunes en el mundo del marketing, que utiliza frases como éstas:

- "¡Compre ahora!"
- "¡Actúe!"
- "¡Sígame!"

En los desbordamientos de búfer informáticos el usuario malintencionado utiliza lo que puede denominarse como un "acolchamiento", que es un método que consiste en añadir algunos caracteres que no interrumpen la ejecución del programa y dejan una "pista de aterrizaje" para amortiguar o "acolchar" la entrada del código malicioso. En ingeniería social se pueden utilizar frases que "acolchen" el lugar donde aterrizará la siguiente orden, como por ejemplo:

- "¿Cómo te sientes cuando..."
- "Una persona puede..."
- "Como puedes..."

Estas palabras crean una emoción o pensamiento que le permitirá introducir código en el subconsciente.

Existen muchos ejemplos de órdenes incrustadas. Repasemos algunos de ellos:

- **Utilizar citas o relatos:** EL cerebro tiende a procesar los relatos de forma distinta a otro tipo de información. Algunos de los mejores maestros que han existido (Aristóteles, Platón, Gamaliel, Jesús) utilizaban relatos para enseñar a quienes les escuchaban. ¿Por qué?

  La mente inconsciente procesa los relatos como instrucciones directas. Bandler, uno de los padres de la PNL, enseña a los profesionales de la PNL a utilizar citas. Sabe que el empleo de citas y relatos le da al orador poder sobre el pensamiento de los oyentes. Puede hacer un uso muy poderoso de esta técnica leyendo citas, utilizándolas e insertando órdenes en ellas.

  Por ejemplo, en cierta ocasión tenía que manipular a un objetivo para que me diera una contraseña antigua para poder "cambiarla" por una más segura. Mi pretexto era ser un técnico de mantenimiento. Enseguida me preguntó qué necesidad había de cambiar de contraseña. Le dije: "Un estudio reciente de la empresa Xavier Research Inc. afirma que el 74 por 100 de las personas utiliza contraseñas poco seguras. Por ese motivo, hemos iniciado este proyecto para cambiar las contraseñas en todas las empresas. Yo me

encargo de cambiar la suya; necesito que me dé su antigua contraseña de Windows y hago el cambio por usted". Al citar una investigación añadí peso a mi argumento.

- **Emplear la negación:** Ésta es una técnica de psicología inversa. Al decirle varias veces al objetivo que no haga algo, puede introducir una orden en la frase. Por ejemplo, si le digo: "No pase mucho tiempo practicando el uso de órdenes incrustadas", estoy deslizando la orden "practique el uso de órdenes incrustadas" dentro de la frase. Además, puedo dar por supuesto que va a practicar hasta cierto punto y si es una persona testaruda puede contestarme: "No me diga lo que tengo que hacer. Practicaré todo lo que me apetezca".
- **Forzar al oyente a utilizar la imaginación:** Este método funciona cuando formula una pregunta empleando frases como "¿qué pasaría..." o "¿cómo se siente si...", en las que el oyente tiene que imaginar algo para poder contestar. Si pregunta: "¿Qué hará cuando sea rico y famoso?", el oyente debe imaginar esa situación para contestarle. Si le pregunto: "¿Qué sucederá cuando domine el uso de las órdenes incrustadas?", le estoy forzando a que se imagine a sí mismo como un maestro de esta técnica y a que piense lo que sentirá entonces. Véalo de esta manera. Si le digo: "No piense en una vaca roja", primero pensará en una vaca roja para después obligarse a no pensar en ella. Su mente inconsciente interpretará cada palabra de la orden para representarla y darle sentido.

  Para cuando su cerebro ha comprendido la frase, su subconsciente ya la ha imaginado. El subconsciente procesa las afirmaciones directamente, sin tener en cuenta el contexto. Otro punto importante es que el subconsciente puede registrar el lenguaje corporal, las expresiones faciales, los tonos de voz y los gestos y conectar esta información con el mensaje hablado. Al unir todas las partes, el subconsciente no tiene otra opción más que obedecer una orden incrustada si la hay.

Cuando emplee las órdenes incrustadas es importante utilizar correctamente los tonos de voz. Si pone demasiado énfasis en las palabras, sonará raro y asustará al objetivo en lugar de insertarle una orden. Al igual que el desbordamiento de búfer informático, la información debe ser coherente con la orden que quiere introducir.

Resumen

Como probablemente ya habrá imaginado, la incrustación de órdenes es un campo muy amplio con mucho margen de error. Debe practicar para dominarlo. Aunque no promuevo el uso de esta información para emplearla en el área de la

seducción, existen algunos vídeos interesantes que explican cómo introducir órdenes para seducir a otra persona. Al utilizar estos principios se crea un ambiente en el que el objetivo es muy receptivo a sus sugerencias.

Simplemente por decirle a alguien: "Vas a comprar lo que te ofrezco", no significa que lo vaya a hacer. Entonces, ¿por qué emplear estas órdenes?

La razón es que crean una plataforma que hace más sencilla la ingeniería social. También son una buena manera de enseñar a las empresas con las que trabaja a estar atentas a las personas que pueden intentar utilizar estas tácticas contra ellas.

Si desarrollara el principio de las órdenes incrustadas como si fuera una ecuación, quedaría de este modo:

Desbordamiento de búfer humano = ley de las expectativas + acolchado + códigos incrustados.

Inicie una conversación con su objetivo utilizando frases y un lenguaje corporal basado en suposiciones. Cuando introduzca una petición presuponga que ya es un hecho consumado.

Después, "acolche" la mente humana con afirmaciones que faciliten la introducción de órdenes. Ésta es la ecuación del desbordamiento de búfer humano. Utilícela con moderación y practique mucho antes de intentarlo. Pruébela en casa o en el trabajo. Elija un objetivo en su oficina que normalmente no accedería a una petición sencilla e intente que le sirva un café: "Tom, vas la cocina, ¿verdad? ¿Puedes traerme un café con leche, por favor?".

Vaya aumentando la magnitud de sus órdenes para ver hasta dónde puede llegar. Utilice esta ecuación para obligar a las personas y comprobar cuánta información puede obtener y cuántas órdenes es capaz de insertar.

En este capítulo se han explicado algunos de los principios psicológicos más asombrosos de la ingeniería social. Estos conceptos pueden cambiar su vida. Comprender cómo piensa la gente, por qué piensa de cierta forma y cómo influir en sus pensamientos es un aspecto muy poderoso de la ingeniería social. Pasamos ahora al siguiente punto de la lista: cómo influenciar a su objetivo.

6. La influencia: el poder de la persuasión

Para persuadir debe apelar al interés, más que al intelecto.
Benjamin Franklin

Este epígrafe sintetiza el capítulo entero. Puede que se pregunte por qué no he incluido este tema en el capítulo 5 con los principios psicológicos de la ingeniería social. La psicología es una ciencia y un grupo de normas que, cuando se cumplen, producen un resultado. Es científica y calculada.

La influencia y la persuasión son más parecidas a un arte respaldado por la ciencia. Implican emociones y creencias. Como hemos explicado en capítulos anteriores, debe saber cómo y qué piensan las personas.

La influencia y el arte de la persuasión es el proceso de lograr que alguien "quiera" reaccionar, pensar, actuar o creer del modo en que "usted" quiere que lo haga.

Lea de nuevo la frase anterior si es necesario. Probablemente, es una de las frases más poderosas de este libro. Significa que, empleando los principios explicados aquí, conseguirá que alguien quiera pensar, actuar e incluso creer como usted quiera. Los ingenieros sociales utilizan el arte de la persuasión a diario y, desgraciadamente, los estafadores también lo hacen.

Mucha gente ha dedicado su vida a investigar, estudiar y perfeccionar el arte de la influencia. Algunos como la doctora Ellen Langer, Robert Cialdini y Kevin Hogan han contribuido con un gran repositorio de conocimiento en este campo. Uniendo este material con las investigaciones y enseñanzas de los maestros de la PNL (programación neurolingüística) como Bandler, Grinder y más recientemente Jamie Smart, conseguirá la receta para convertirse en un auténtico artista de la persuasión.

La influencia auténtica es elegante y sutil y casi siempre indetectable para quienes están siendo influenciados. Cuando aprenda los métodos empezará a detectarlos en la publicidad y en las estrategias de los vendedores. Empezarán a molestarle los intentos chapuceros de la gente del marketing y, si se parece a mí, empezará a poner el grito en el cielo cuando vea anuncios horribles en la televisión y las vallas publicitarias (una costumbre que mi mujer no aprecia demasiado).

El capítulo comienza con un pequeño repaso a ciertos elementos clave de la persuasión y la influencia que he reunido y utilizado. Se explican conceptos como la reciprocidad, la manipulación y el poder de establecer metas, por nombrar algunos.

La influencia y la persuasión se pueden desglosar en cinco aspectos importantes, como se explica en las siguientes secciones.

Los cinco fundamentos de la influencia y la persuasión

Los cinco fundamentos de la persuasión son vitales para influir con éxito en un objetivo:

- Establecer metas claras.
- Crear compenetración.
- Ser observador con lo que le rodea.
- Ser flexible.
- Entrar en contacto consigo mismo.

La meta final de la ingeniería social es influenciar al objetivo para que realice una acción que puede no ir en su propio interés. Es más, no consiste sólo en que realice la acción sino en que "quiera" realizarla e incluso le dé las gracias por ello. Este tipo de influencia es muy poderosa y convierte en leyendas a los profesionales que la dominan.

El famoso instructor de PNL Jamie Smart dijo una vez: "El mapa no es el terreno". Me encanta esta cita porque encaja perfectamente con estos cinco fundamentos. Ninguno de ellos lo abarca todo por sí solo, pero cada uno es como un punto en un mapa que le muestra el terreno completo de lo que quiere conseguir. La siguiente sección profundiza en el primer fundamento: por qué es tan importante establecer metas claras.

Tenga en mente una meta clara

No sólo debe tener la meta en su cabeza, debe escribirla. Pregúntese: "¿Qué es lo que quiero lograr de esta interacción?".

Como expliqué en el capítulo 5, sobre todo en relación a la PNL, los sistemas internos del ser humano se ven afectados por sus pensamientos y aspiraciones. Si concentra su energía en lograr algo, es probable que lo consiga. Esto no significa que si se concentra en conseguir un millón de euros lo vaya a lograr. De hecho, es muy poco probable. Sin embargo, si tiene la meta de llegar a ganar un millón de euros y se centra en los pasos que debe dar para conseguirlo, sus acciones aumentarán las probabilidades de que lo consiga. Lo mismo ocurre con la persuasión. ¿Cuál es su meta? ¿Cambiar las creencias de alguien? ¿Conseguir que realice una acción? Imagine que un amigo íntimo está haciendo algo muy perjudicial para él y quiere convencerle de que lo deje. ¿Cuál es la meta en este caso? Puede que la meta final sea persuadirle de que lo deje, pero quizá sea necesario establecer pequeñas metas por el camino. Definir esas metas puede hacer más clara la estrategia para influenciar a esta persona. Después de definir la meta debe preguntarse: "¿Cuándo sabré que he conseguido lo que quiero?". En cierta ocasión, escuché un programa de formación ofrecido por Jamie Smart, uno de los líderes en PNL, en el que les hacía a todas las personas de la clase estas dos preguntas:

- ¿Qué es lo que quiere?
- ¿Cómo sabrá cuándo lo ha conseguido?

En ese momento, detuve el CD en la primera pregunta y contesté en voz alta lo que quería de ese curso. Continué viendo el vídeo y, cuando se formula la segunda pregunta, "¿cómo sabrá cuándo lo ha conseguido?", detuve otra vez el CD y no supe qué contestar. Estaba claro que me faltaba un mapa. Sabía lo que quería del curso pero no sabía cómo determinar cuándo lo había conseguido. Saber lo que se quiere es un aspecto importante de las tácticas de persuasión e influencia. Cuando aborda a un objetivo sabiendo cuál es su meta y cuáles son las señales que le indicarán que lo ha logrado, entonces puede diseñar claramente el camino a seguir. Definir las metas con precisión es fundamental para el éxito de las tácticas de persuasión y ayuda a dominar el siguiente paso.

Compenetración, compenetración, compenetración

En el capítulo 5, encontrará toda una sección explicando el concepto de la creación de compenetración. Estúdiela y perfeccione sus habilidades para lograrlo.

Desarrollar compenetración implica atraer la atención del objetivo y de su subconsciente y generar confianza en ese plano inconsciente.

Dominar esta técnica puede cambiar el modo en que se relaciona con los demás y toda su metodología a nivel profesional.

Para crear compenetración, empiece por el punto en el que se encuentra su objetivo mentalmente. Intente comprender su estado mental. ¿Es desconfiado? ¿Está triste, disgustado o preocupado? No se centre tanto en sus propias metas, sino en comprender a esta persona. Éste es un punto fundamental. Un ingeniero social debe entender a su objetivo lo suficiente como para saber en qué estado se encuentra a nivel consciente. ¿Cuáles son sus pensamientos y su estado mental?

Por ejemplo, imagine que quiere influenciar a su amigo para que deje el tabaco o las drogas o algún otro hábito perjudicial. Tenga en cuenta que no tiene que convencerle de que lo deje, sino convencerle para que "quiera" dejarlo. La meta tiene que enfocarse en el objetivo, no en usted. No puede iniciar la conversación diciendo lo que su adicción le preocupa a "usted", lo mucho que le molesta el olor, etc. El argumento tiene que girar alrededor del objetivo. No puede empezar con un ataque verbal sobre lo mucho que le disgusta su problema. Tiene que entender su estado mental, aceptarlo y alinearse con él.

En ingeniería social ocurre lo mismo: no puede empezar por el punto en el que está usted mentalmente. Esto puede ser complicado para mucha gente. ¿Sabe por qué fuma? ¿Conoce las razones psicológicas, físicas o mentales? Hasta que no consiga ponerse en su lugar, no podrá compenetrarse con él y su intento de influenciarlo fracasará.

Por otra parte, no siempre puede basar la compenetración en la lógica. En cierta ocasión, estaba en el hospital con un amigo que estaba muriendo de cáncer de garganta. Había fumado durante más de cuarenta años hasta que un día descubrió la enfermedad. El cáncer se extendió con rapidez y acabó pasando sus últimos días ingresado en el hospital. Sus hijos venían a visitarle y de vez en cuando salían de la habitación. Pensé que lo hacían porque la emoción les superaba. Una de las veces que salieron fui tras ellos para tratar de consolarlos y los encontré en el exterior del hospital ¡fumando! Me quedé estupefacto. Yo no fumo, nunca me ha apetecido y, aunque puedo comprender lo fuerte que puede ser una adicción, no entendía cómo, después de ver el sufrimiento por el que estaba pasando su padre, podían llevarse un cigarrillo a los labios.

La lógica no servía en este caso. Decirle a estos chicos que el tabaco es malo y que les acabaría matando no serviría de nada. Sería una información inútil que sólo conseguiría hacerme sentir bien por decirla, pero que no estaría alineada con su estado mental actual. Hasta que no entiende a la persona no puede crear una buena compenetración para influenciarla.

Conseguir que alguien quiera realizar una acción es una mezcla de emociones y lógica, así como de comprensión y humanidad en muchos casos. En una ocasión, estaba entrando en una oficina en la que tenía que hacer un trabajo. Había escuchado un comentario gracioso en el exterior, así que cuando entré todavía me estaba riendo. La mujer de recepción debía de haber hecho algo embarazoso justo antes porque cuando me vio se enfadó de inmediato y me gritó: "No tiene ninguna gracia, eres un idiota".

No conocía a esta mujer y, a decir verdad, tenía un plan en mente que no iba a funcionar después de este encuentro. Además, me sentí ofendido porque pensara que me estaba riendo de ella y estaba deseando devolverle el golpe. Sin embargo, observé que estaba disgustada. Me acerqué al mostrador para que no me oyera nadie más, la miré a los ojos y le dije sinceramente: "Lo siento si ha pensado que me reía de usted. Unos compañeros suyos han contado una anécdota graciosa en el aparcamiento y por eso me estaba riendo".

Me miró y noté que ahora estaba incluso más avergonzada, así que para sacarla del apuro dije en voz alta: "Señora, siento haberme reído y haberla avergonzado". Esto le hizo quedar bien con la gente que teníamos alrededor. Comprendió que me había sacrificado por ella y respondió con mucha amabilidad. Un minuto después se disculpó conmigo y me beneficié enormemente del asunto porque conseguí toda la información que iba buscando y con mucho menos esfuerzo de lo normal.

Un profesor que tuve solía decir: "Mátalos de amabilidad". Ésta es una afirmación bastante significativa. Ser amable es una forma rápida de crear compenetración y establecerse en los cinco fundamentos de la persuasión.

Un método para influenciar a la gente empleando la amabilidad y la compenetración es hacer preguntas y dar opciones que conduzcan al camino que desea. Por ejemplo, en una ocasión me vi influenciado a realizar una labor que no quería como parte de un trabajo de equipo. El líder del grupo era muy carismático y amable y tenía un encanto personal que le permitía hablar con cualquiera. Se me acercó y me dijo: "Chris, quería hablar contigo en privado. Necesito una persona que sea mi mano derecha en un pequeño proyecto. Pero tiene que ser una persona ambiciosa y motivada. Creo que esa persona eres tú, pero no quiero anticiparme; ¿tú que piensas?".

Me sentí entusiasmado por los halagos y la oportunidad de ser "importante", por lo que respondí: "Soy una persona con mucha motivación. Cualquier cosa que necesites, dímelo".

El líder continuó: "Verás, creo firmemente en la idea de pregonar con el ejemplo. Creo que tienes cualidades de liderazgo. El problema es que algunos compañeros del grupo no lo creen y necesitan a alguien fuerte que les guíe".

Antes de que acabara la conversación consiguió que lo que él quería surgiera como si hubiera sido idea mía, por lo que no podía echarme atrás. Fue muy convincente, desde luego, y todo empezó con el poder de la persuasión.

Conecte con usted mismo y con lo que le rodea

La agudeza sensorial es la habilidad para detectar las señales en su objetivo y en usted que le indican si se está moviendo en la dirección adecuada.

Muchos de los principios explicados en el capítulo previo son aplicables a la persuasión. Leer el lenguaje corporal y las expresiones faciales pueden decirle mucho sobre su influencia sobre el objetivo.

Para dominar de verdad el arte dual de la influencia y la persuasión debe convertirse en un maestro escuchando y observando. Chris Westbury, un neuropsicólogo cognitivo de la Universidad de Alberta en Canadá, calcula que el cerebro humano procesa información a una velocidad de 20 mil billones de cálculos por segundo. Esos cálculos se representan a través de expresiones faciales, microexpresiones, gestos, posturas, tonos de voz, parpadeos, ritmo respiratorio, patrones lingüísticos, expresiones no verbales y muchos otros patrones distintivos. Dominar la persuasión implica ser consciente de estas sutilezas en usted y en los demás.

En mi caso, la habilidad de ser observador me resultó más fácil después de recibir formación en microexpresiones por parte del doctor Ekman. Descubrí que no sólo era mucho más consciente de lo que sucedía a mí alrededor, sino también de mí mismo. Cuando sentía cierta expresión en mi rostro la analizaba y pensaba cómo podía representarla para los demás. Este reconocimiento de mí mismo y de mi alrededor fue una de las experiencias más instructivas de mi vida.

Los expertos en PNL recomiendan minimizar el diálogo interno cuando intente influenciar a otros. Si cuando interactúa con el objetivo está pensando en la siguiente fase del ataque, en la meta final o en cómo superar una posible barrera comunicativa, ese diálogo interno puede provocar que pase por alto mucho de lo que sucede a su alrededor. Ser observador cuesta trabajo, pero tiene recompensa.

No sea insensato: sea flexible

¿Qué quiere decir que no sea insensato y que sea flexible? Una antigua definición de la insensatez es "hacer lo mismo una y otra vez y pretender obtener resultados diferentes". Una de las claves de la persuasión es la flexibilidad y la disponibilidad.

Persuadir es como doblar la voluntad. Si tuviera la tarea de doblar algo, ¿Qué preferiría doblar? ¿La rama de un sauce o una barra de acero? Lógicamente es preferible la rama de sauce porque es flexible, fácil de doblar. Intentar persuadir a alguien con una actitud rígida e inflexible no funciona, como tampoco es sencillo persuadir a alguien si usted no es flexible.

A menudo, una auditoría no saldrá como se ha planeado. Un buen ingeniero social será capaz de encajar los golpes y ajustar sus metas y sus métodos a las necesidades. Esto no contradice la idea de planear con antelación; más bien denota la importancia de no ser rígido para poder adaptarse a los cambios y lograr su meta.

La forma en que una persona ve a un insensato es la forma en que un objetivo ve a un ingeniero social inflexible. Si aparece como una persona poco razonable a los ojos del objetivo, es probable que no consiga lo que quiere.

Contacte con usted mismo

No estoy sugiriendo que se dedique a la meditación zen, simplemente que comprenda sus emociones. Las emociones controlan prácticamente todo lo que hace, así como todo lo que hace su objetivo. Conociéndose a sí mismo, logrará preparar el terreno para llegar a ser un auditor efectivo.

Volviendo al ejemplo del amigo fumador, si usted siente un odio profundo por los fumadores, esto le afectará en su interacción con su amigo. Puede hacer que diga o haga algo que cierre la puerta a la persuasión. Es posible que haya cosas en las que nunca podrán estar de acuerdo. Ser consciente de cuáles son esas cosas y de sus sentimientos hacia ellas le ayudará a definir un camino claro para influenciar al objetivo.

Estos cinco fundamentos son clave para comprender la influencia y la persuasión. La meta de la persuasión es ser capaz de crear un ambiente en el que el objetivo desee llevar a cabo lo que le pide y estos cinco fundamentos le ayudarán a crear ese ambiente. La siguiente sección explica cómo emplear estos fundamentos.

Las tácticas de influencia

Como ya hemos comentado, la técnica de la persuasión debe practicarse hasta que se convierta en un hábito. Esto no significa que debe influenciar a todo el mundo en todo lo que haga, sino en tener esta técnica siempre preparada para utilizarla cuando la ocasión lo requiera.

Hay varios aspectos de la influencia y la persuasión que puede emplear y muchos de ellos encajan a la perfección en una auditoría de seguridad. Otros aspectos no encajan tan fácilmente, pero son fundamentales en el campo de la influencia. Las siguientes secciones explican ocho técnicas diferentes de influencia utilizadas a menudo por los medios de comunicación, los políticos, los gobiernos, los estafadores, los timadores y, por supuesto, los ingenieros sociales.

Cada sección proporciona un análisis de cada técnica para comprobar cómo se emplea en ingeniería social y en otros ámbitos.

Reciprocidad

La reciprocidad es un sentido de correspondencia inherente que provoca que cuando alguien nos trata bien respondamos del mismo modo.

Un ejemplo sencillo se da cuando al entrar en un edificio alguien le sostiene la puerta abierta. Esa persona esperará que le dé las gracias y que abra la siguiente puerta para ella.

La regla de la reciprocidad es importante porque a menudo la devolución del favor se hace de manera inconsciente. Sabiendo esto, ya ha dado un paso importante para poder utilizarla como ingeniero social. Pero, antes, repasemos algunos ejemplos en los que habitualmente se emplea la reciprocidad:

- Las empresas farmacéuticas gastan entre 10.000 y 15.000 euros por médico (sí, por médico) en "regalos" que pueden consistir en cenas, libros, ordenadores, trajes u otros objetos con el logo de la empresa en ellos. Cuando llega el momento de recetar un medicamento, ¿cuál cree que es más probable que elija el médico?
- A todos los políticos se les influye de una forma muy parecida. No es ningún secreto que habitualmente los políticos y los grupos de presión favorecen más a las personas que apoyaron sus campañas que a las que no lo hicieron.
- La reciprocidad se emplea a menudo en el mundo de los negocios, sobre todo en lo que se refiere a los contratos. Puede que el comercial invite a una comida y después pida una concesión en el contrato. El cliente se verá forzado a ceder la concesión.
- Un compañero de trabajo le sustituyó cuando necesitaba tomarse un día libre. Ahora le pide que le devuelva el favor pero usted tiene planes. En esta situación, la mayoría de la gente cambiará sus planes para cumplir con la petición.

Todos estos son ejemplos de reciprocidad. Alvin Gouldner escribió un artículo llamado "The Norm of Reciprocity" (La regla de la reciprocidad), que puede consultar en `http://media.pfeiffer.edu/lridener/courses/normecp.html`, en el que afirma:

De manera especifica sugiero que la regla de la reciprocidad, en su forma general, contenga dos exigencias mínimas e interrelacionadas: (1) la gente debe ayudar a quien le ha ayudado y (2) la gente no debe herir a quien le ha ayudado. De forma general, la regla de reciprocidad puede concebirse como una dimensión que se encuentra en todos los sistemas de valores y, en particular, como uno entre varios de los "componentes principales" presentes globalmente en los códigos morales.

Básicamente, su investigación le condujo a la conclusión de que la reciprocidad funciona independientemente de los orígenes culturales. Bajo las circunstancias adecuadas, la reciprocidad es prácticamente imposible de evitar.

Piense en la reciprocidad como el proceso que se ilustra a continuación en la figura 6.1.



Figura 6.1. *El ciclo de la reciprocidad.*

Las siguientes secciones explican algunos puntos clave de esta idea.

Dar algo

Lo que se entrega no puede ser algo sin valor, debe ser algo valioso para el receptor. Regalar una preciosa novela en tapa dura escrita en un idioma que el receptor no sabe leer es inútil.

Lo que se entrega puede ser un servicio, un objeto, una información importante, ayuda o cualquier otra cosa valiosa para el receptor (incluso algo aparentemente sencillo como sostener la puerta para que pase o recoger algo que se la ha caído al suelo). En el mundo del marketing, se utiliza habitualmente este método pero muchas veces se quedan cortos porque ofrecen cosas que no tienen ningún valor. Imagine que está en una feria comercial y en cada puesto las distintas empresas hacen regalos a la gente. Si llega a un puesto y ve que regalan unos bolígrafos baratos, puede que pase de largo. En el siguiente tienen un interesante puzle. Siente curiosidad y lo coge; después de pasar unos minutos jugando con él, se le acerca un comercial y le dice: "¿Quiere una pista para resolverlo?". Después de enseñarle una pequeña pista, le pregunta si tiene un minuto para que le presente un servicio que puede interesarle.

¿Cómo negarse? Le han dado un juego curioso y una pequeña ayuda para resolverlo y ahora sólo le piden un minuto de su tiempo. Lo han organizado a la perfección.

El sentimiento de estar en deuda

Cuanto más valor tenga el regalo para el receptor y cuanto más inesperado sea, mayor será el sentimiento de deuda que tenga.

Es importante no utilizar el regalo en una táctica de manipulación evidente. No diga algo como "te he regalado esto así que ahora me debes una". Incluso si lo piensa puede provocar que desaparezca el sentimiento del receptor de estar en deuda. El "regalo" debe ser totalmente gratis y tener mucho valor para el receptor.

La Humane Society (Asociación humanitaria) de Estados Unidos regala etiquetas personalizadas para el correo. Las entregan sin ningún compromiso y mucha gente las utiliza para sus cartas personales. Son bonitas y de buena calidad. Para recibirlas, hay que registrarse y muchos meses después se recibe una llamada pidiéndole colaboración con una donación. El receptor suele sentirse emocionalmente obligado a realizar al menos una pequeña contribución.

A modo de ejemplo, la revista *Fortune Magazine* ofrece a los profesores de universidad ejemplares de la revista para que las utilicen en sus clases, sin compromiso.

Existen muchos casos de reciprocidad como éstos. La otra cara de la moneda son las empresas que se equivocan creyendo que regalos como éstos son buenos para generar reciprocidad:

- Folletos corporativos llamativos y a todo color.
- Juguetes baratos e inútiles.
- Prospectos sobre sus productos o sobre la empresa.

Estas cosas no generan un sentimiento de estar en deuda. El regalo debe ser valioso para el receptor. Un tipo de "regalo" que verdaderamente provoca el sentimiento de deuda es la información. Revelar una información útil, valiosa o beneficiosa puede ser mucho más efectivo que entregar un regalo físico.

Realizar la petición

En cierta ocasión, me disponía a entrar en el edificio de una empresa y vi a un hombre que tenía toda la pinta de ser el "jefe". Salía de su coche recién aparcado en la plaza marcada con el cartel "reservado para el director general" y hablaba por su teléfono móvil. No estaba de buen humor y escuché que estaba disgustado porque tenía que despedir a algunas personas. Me dio la sensación de que estaba hablando con su pareja y que no le gustaba lo que se disponía a hacer.

Le adelanté y me acerqué al mostrador donde la recepcionista estaba jugando al "buscaminas" con el ordenador. Me recibió con el típico "¿qué puedo hacer por usted?", pero su mirada indicaba que estaba aburrida y desganada. Dije: "Verás, vengo a una cita, pero tu jefe estaba a punto de entrar y viene de muy mal humor...". Dejé de hablar y me quedé quieto. Unos segundos después, el jefe entró por la puerta y dije en voz alta: "Muchas gracias por su ayuda".

La recepcionista me miró y dijo: "Perdone un momento, señor" y después le dijo al jefe: "Buenos días, señor Smith, aquí tengo sus mensajes" y le entregó una pequeña pila de papeles antes de que se alejara.

Cuando se fue el jefe, la recepcionista me dio las gracias efusivamente. La había salvado y ella lo sabía. La información que le había dado era muy valiosa y ahora podía formular mi petición: "Necesito tu ayuda. Tengo que ver a la directora de recursos humanos. Sólo será un momento. ¿Puedes llevarme a su despacho?".

Me llevó hasta el despacho de la directora y me presentó como "un amigo" suyo que pasaba por allí. En unos minutos mi plan estaba en marcha y todo gracias a la reciprocidad.

Debe buscar las pequeñas oportunidades para revelar información valiosa para el receptor y, lo que es más importante, lograr que el receptor se sienta en deuda con usted.

Fíjese en todo lo que le rodea y en los pequeños detalles que pueden hacer que un objetivo se sienta obligado a devolverle un favor. Recuerde que no es necesario que sea algo impresionante, simplemente algo que tenga cierto valor para el objetivo.

Es importante tener en cuenta que no debe "acosar" al objetivo. Mirarlo fijamente esperando una oportunidad para hacer o decir algo puede resultar molesto. Debe actuar con naturalidad.

La naturalidad implica que empiece a poner en práctica estos principios en su día a día. Sostenga la puerta para los demás, sea cortés y busque oportunidades para hacer cosas buenas por los demás. Empezará a realizar estas acciones con toda naturalidad y resultarán mucho más sencillas cuando las aplique en una auditoría.

La reciprocidad es una poderosa táctica de influencia. A continuación, se explican dos principios íntimamente relacionados con ella.

El compromiso

El compromiso se refiere a las acciones que uno siente que debe llevar a cabo debido a algún tipo de requerimiento social, legal o moral o debido a una obligación, contrato o promesa. En el contexto de la ingeniería social, el compromiso se relaciona directamente con la reciprocidad pero no se limita a ella. El compromiso puede ser tan sencillo como sostener la puerta para alguien, que normalmente hará que esa persona sostenga la siguiente puerta para usted.

En un plano más serio, puede consistir en que alguien le revele información privada porque ha provocado que se sienta obligado a hacerlo. El compromiso es un vector de ataque habitual cuando el objetivo es el personal de atención al cliente.

También puede emplear el compromiso en pequeñas dosis haciendo cumplidos. Por ejemplo, puede dedicar un cumplido al objetivo y después formular su petición. Esta técnica puede emplearse mal con facilidad si no tiene experiencia, dándole al objetivo una sensación de falsedad que le alertará, produciéndose un resultado negativo. No obstante, si se efectúa adecuadamente, puede servir para obtener información muy valiosa.

Un ejemplo de un cumplido mal formulado sería decir: "Vaya, qué ojos más bonitos, ¿puedo entrar en el cuarto del servidor?". Suena estúpido, ¿verdad? Pruebe sus frases diciéndolas en voz alta para comprobar cómo suenan. Si parecen frases de mal gusto para ligar, descártelas.

Por otro lado, una pequeña conversación como la que sigue puede ser una buena manera de hacer un cumplido.

Al llegar a la mesa de recepción observa unas fotos de unos niños pequeños en Disney World y, después de presentarse, dice: "¿Ésos son sus hijos? Qué guapos son". No importa si los chicos son sus hijos o sus sobrinos, seguro que le gusta el cumplido. Después continúa diciendo: "Yo también tengo dos. Le mantienen a uno joven, ¿verdad?".

"Sí, son mis hijos. Aunque no estoy segura de que me hagan sentir joven", dice ella sonriendo. "A mí me agotan".

"Yo aún no he llevado a los míos a Disney World", dice. "¿Cree que a esa edad lo disfrutan de verdad?".

"Oh, sí. Los míos disfrutaron de cada segundo que pasaron allí", dice la recepcionista. "Mientras mi hija esté con su querido papi, se lo pasa bien".

"Ah, sí, yo también tengo una pequeña princesita. Bueno, la verdad es que podría pasar aquí todo el día hablando de mis hijos, pero me preguntaba si podría ayudarme con un asunto. Llamé hace una semana y hablé con alguien sobre un nuevo software de recursos humanos y dije que vendría a dejar aquí en la oficina la información pero he perdido el papel donde apunté el nombre de esa persona, que vergüenza".

"Ah, seguramente se trate de la señora Smith", dice la recepcionista". "Ella se encarga de esos asuntos".

"Me ha salvado la vida. Le debo una. Muchas gracias".

Este tipo de cumplidos ayudan mucho a abrir al objetivo para que sea más susceptible a la influencia.

La regla de oro es: trate a los demás como le gustaría que le trataran a usted. Es un principio clave para generar compromiso. Tratar a la gente con amabilidad y darles algo que pueden necesitar, aunque sea un pequeño cumplido, puede crear un sentido de compromiso hacia usted.

El psicólogo Steve Bressert confirma este punto en su artículo "Persuasion and How To Influence Others" (La persuasión y cómo influenciar a los demás) en el que afirma: "Según la organización American Disabled Veterans (Veteranos discapacitados de Estados Unidos), enviar una simple solicitud de donativos produce una tasa de éxito del 18 por 100. Acompañándola con un pequeño regalo, como unas tarjetas personalizadas para el correo, la tasa de éxito aumenta al 35 por 100: 'Como me envían estas útiles tarjetas, les envío una pequeña donación a cambio'".

Si quiere comprobar el poder de este principio, pruebe este sencillo ejercicio. Incluso algo tan pequeño como una pregunta puede generar compromiso. La próxima vez que alguien le haga una pregunta no diga nada. Permanezca en silencio o ignórela y continúe con la conversación. Observe lo incómodo que resulta; algo tan sencillo como una pregunta crea un sentido de compromiso por responder. Simplemente haciendo una pregunta al objetivo puede obtener resultados increíbles.

Si con su primera acción ha provocado la sensación de que debe haber un seguimiento posterior, entonces cumplir esa expectativa puede generar un fuerte sentido de compromiso. Cuando la persona con la que interactúa espera cierto resultado, si lo cumple provocará un fuerte compromiso en ella por hacer lo mismo por usted.

Este método puede utilizarse, por ejemplo, enviando al director de finanzas de una empresa un aparato tecnológico, como un iPod, cargado con software malicioso. Al recibir el regalo sentirá el compromiso de conectarlo. Una acción de

ataque que he visto tener éxito en varias ocasiones es enviar un regalo al director general con una tarjeta que diga: "Por favor, acepte este pequeño regalo de nuestra empresa. Sólo le pedimos que consulte nuestros productos en `www.products.com` y descargue nuestro catálogo en PDF en `www.products.com/catalog.pdf`. Le llamaré la semana que viene".

Este método siempre funciona.

La concesión

La concesión o el acto de conceder se define como "un reconocimiento o admisión" o "el acto de ceder". La concesión se utiliza a menudo para incidir sobre el instinto de reciprocidad de los seres humanos. Parece que tenemos una función incorporada que nos hace querer "hacer a los otros lo que ellos nos hacen". Un auditor de seguridad puede sacar partido de la idea de "cambiar una cosa por otra" o el principio de "te rasco la espalda si rascas la mía". Existen ciertos principios básicos sobre la concesión y cómo utilizarla de forma adecuada:

- **Marque sus concesiones:** Haga saber qué y cuándo está haciendo una concesión. De esta forma, conseguirá que sea difícil para su objetivo olvidar la necesidad de corresponder. Es necesario cierto equilibrio porque no debe "lanzar las campanas al vuelo", por decirlo así. Una afirmación del tipo "de acuerdo, te doy la razón en esto" o "está bien, lo acepto" muestra que está dispuesto a conceder.
- **Exija y defina la reciprocidad:** Puede empezar plantando las semillas de la reciprocidad, de este modo aumentará las posibilidades de obtener algo a cambio. Una forma sencilla de plantar esas semillas es a través de la comunicación no verbal, mostrando que es una persona flexible y sabiendo escuchar. Estos detalles marcan la diferencia a la hora de generar reciprocidad en su objetivo.
- **Haga concesiones contingentes:** Puede hacer concesiones de "bajo riesgo" cuando haya poca confianza o cuando necesite enviar el mensaje de que está dispuesto a hacer otras concesiones. Éste es un tipo de concesión que no va unida a una actitud del tipo "ahora usted puede hacer algo por mí". Cediendo a algo que el objetivo necesita o quiere sin esperar nada a cambio forma un estrecho vínculo con él.
- **Haga concesiones a plazos:** La idea de la reciprocidad está arraigada profundamente en nuestras mentes. La mayoría de la gente piensa que si se le hace un favor está socialmente comprometido a devolverlo. Del

mismo modo, si alguien hace una concesión en una negociación, la otra parte se siente instintivamente obligada a ceder un poco también. Teniendo en cuenta este hecho, no debe sentir la necesidad de hacer todas sus concesiones al mismo tiempo. Puede dividir sus concesiones en "plazos", dando un poco aquí y un poco allí para mantener a su objetivo correspondiéndole.

Las concesiones se emplean a diario por vendedores, negociadores e ingenieros sociales. Un buen auditor de seguridad puede usar y abusar de esta tendencia instintiva, no sólo resistiéndose a las manipulaciones a las que intenten someterle, sino también intentando asumir completamente el control de la situación.

La concesión y la reciprocidad funcionan bien junto a otras técnicas explicadas en este libro.

Un ejemplo que muestra la enorme cantidad de gente que accede a las concesiones puede encontrarse en el telemarketing para pedir donativos. Emplean una estrategia para obtener concesiones que consiste en darle primero al objetivo la opción de rechazar una petición importante. Entonces el solicitante contraataca con una petición más pequeña que el objetivo estará mucho más dispuesto a aceptar.

Petición importante: "¿Podría donar 200 euros para nuestra obra de caridad?".

Respuesta: "No, no puedo".

Petición pequeña: "Oh, lo siento, señor, y lo comprendo. ¿Podría donar tan sólo 20 euros?".

La gente que no conoce esta técnica puede sentir que se ha librado del peso de la petición de 200 euros y considera que puede zanjar el asunto con tan sólo 20 euros.

Otro buen ejemplo apareció en un artículo (`http://ezinearticles.com/?How-to-Negotiate-the-Salary-Using-the-Power-of-the-Norm-of-Reciprocity&id=2449465`) escrito por David Hill:

El poder de esta regla puede verse en la mayoría de negociaciones. Imagine que un comprador y un vendedor están regateando el precio de un coche. El vendedor empieza haciendo una oferta de 24.000 euros. El comprador encuentra inaceptable este precio y realiza una contraoferta de 15.000 euros. Entonces el vendedor baja su oferta a 20.000 euros, por lo tanto hace una concesión. En ese caso, lo normal será que el comprador se sienta inclinado a elevar su oferta, por ejemplo a 17.000 euros. La razón por la que el comprador haría esto es por efecto de la regla de reciprocidad. Esta regla exige que el comprador responda a la concesión del vendedor con otra concesión.

Al igual que la mayoría de principios discutidos hasta ahora, la concesión debe ser valiosa para el receptor. No se puede conceder algo que sólo es valioso para uno mismo o se perderá el valor de este concepto.

También es fundamental no hacer una concesión que le haga quedar mal o perder compenetración o cierta posición. Debe existir un equilibrio entre la concesión y su posición respecto al objetivo y encontrarlo es la mitad de la tarea. Encuéntrelo y la concesión será una herramienta muy poderosa en sus manos.

La escasez

A menudo, la gente encuentra más atractivos objetos y oportunidades si son raros, escasos o difíciles de conseguir. Por este motivo, encuentra habitualmente en los anuncios de la radio y los periódicos mensajes como "últimos días", "oferta por tiempo limitado", "tres días de rebajas" y "liquidación por fin de negocio", que atraen a la gente para intentar conseguir ese producto antes de que desaparezca para siempre.

La utilización de la escasez en un contexto comercial se materializa con un eslogan como "¡Reaccione! ¡Los artículos son limitados!". Otras técnicas incluyen el típico "para las primeras X llamadas, este artilugio de regalo" u ofrecer un suministro intencionadamente escaso de un producto popular. Recientemente, se ha empleado esta táctica con la Nintendo Wii. Jason Dobson, escritor de la revista *Gamasutra*, dijo: "Creo que [Nintendo] dejó que se agotara el suministro intencionadamente para cumplir las cifras del año. La nueva temporada empieza el 1 de abril y me da la sensación de que vamos a ver cómo fluye entonces el suministro" (`www.gamasutra.com/php-bin/news_index.php?story=13297`).

En el lugar donde vivo, un concesionario publicó un anuncio un jueves en el que afirmaban que tenían que deshacerse de cierta cantidad de coches debido a la llegada de nuevo *stock*. Los precios habían bajado mucho y los coches (atención) se habían dejado de fabricar. Ese fin de semana era el último en que podía entrar a forma parte de un pedazo de historia de la venta de coches.

Las ventas se dispararon ese fin de semana y se acabó la oferta, ¿verdad? No, publicaron ese anuncio cada jueves durante los siguientes tres meses. Siempre me pregunté cómo era posible que la gente no se diera cuenta, pero la realidad es que el concesionario vendió muchos coches empleando este método.

Los eventos sociales a menudo resultan más exclusivos si se introduce el elemento de la escasez. El beneficio social percibido de acudir a estos eventos crece en estas circunstancias. En publicidad se emplea este método con los anuncios de eventos musicales en los que se afirma que en el último concierto del grupo se vendieron rápidamente las entradas.

Muchos restaurantes conocidos cierran partes de sus locales para parecer más llenos de lo que lo están. La percepción de que son tan populares hace crecer el deseo de comer allí. Para ver un anuncio que menciona el empleo de la escasez para promocionar un evento, consulte `www.social-engineer.org/wiki/archives/Scarcity/Scarcity-Advertisment.html`.

Este anuncio pone en juego tres elementos fundamentales de la escasez:

- El lanzamiento es de acceso limitado.
- La solicitud no es pública y es limitada.
- Los promotores se escogen a dedo y de forma limitada.
- El libro electrónico es gratis para los afortunados elegidos para asistir.

Todos estos punto utilizan la escasez para crear la sensación en el público de que es tan complicado asistir a este evento que sólo unos pocos, la élite, los elegidos, pueden tener una remota oportunidad de pisar ese lugar sagrado.

Las bases de la economía consisten en la distribución de recursos con usos alternativos. Esta distribución depende de la escasez de los productos en cuestión. Cuanto menos habitual sea el recurso, mayor será el valor otorgado al objeto. Éste es el motivo de que el oro tenga más valor que la sal y que ésta a su vez valga más que la arcilla.

La escasez se utiliza en interacciones todos los días. Puede introducirse en situaciones sociales en un intento de que aumente el valor de algo que una persona posee. Por ejemplo, alguien puede actuar como si estuviera siempre muy ocupado y le costara mucho encontrar tiempo libre.

De esta forma, tiene una excusa para no pasar tiempo con alguien con quien debería pasarlo y, además, consigue que el tiempo que pasa con esa persona parezca mucho más valioso.

Con la escasez también se puede manipular la atención. Piense en las personas que se quejan de que los vendedores les molestan en una tienda cuando hay muchos pero luego les irrita que los vendedores les ignoren cuando escasean. En general, la gente desea lo que es difícil de conseguir porque se asume que tiene más valor. Esto se puede aplicar también a la atención.

La escasez se emplea a menudo en el contexto de la ingeniería social para crear un sentimiento de urgencia en una situación en la que debe tomarse una decisión. Esta urgencia puede servir para manipular el proceso de toma de decisión, permitiendo al auditor controlar la información proporcionada al objetivo. Esto se lleva a cabo normalmente empleando una mezcla de autoridad y escasez. Por ejemplo, diciendo algo como: "El director, el señor Smith, me llamó antes de irse de puente y me dijo que viniera a arreglar su problema con el correo electrónico. Dijo que

estaba harto de que no funcionara y que lo quería arreglado para el lunes". Esto crea una sensación de urgencia y también de escasez, ya que el director no está disponible. El tiempo sería el bien escaso en esta situación.

Al utilizar la escasez junto a otros principios se consigue hacer el ataque aun más letal. En cualquier caso, la escasez provoca deseo y éste puede conducir a alguien a tomar una decisión de la que luego se puede arrepentir.

Comprobé este hecho hace poco tiempo cuando una furgoneta se detuvo en la entrada de mi casa. Un hombre joven y bien vestido se acercó hasta la puerta de casa y le explicó a mi mujer que vendía carne. Había terminado de repartir entre sus clientes y estaba a punto de volver a su local cuando la vio trabajando en el jardín. Empezó a hablar de lo altos que son los precios en las tiendas. Tenía un acento agradable y la llamaba "señora" respetuosamente.

Después de hablar durante unos minutos, mi mujer lanzó la pregunta que normalmente deja helados a los vendedores: "¿Cuánto pide?".

Sin pérdida de tiempo dijo: "Verá, he estado vendiendo esta carne a 400 euros la caja, pero ésta es la última que me queda. Me encantaría volver con la furgoneta vacía y de paso ofrecerle una carne de excelente calidad".

¡Oh no, la última caja! También le había dicho a mi mujer que sólo repartía una vez cada dos meses. Ya había despertado el deseo, pero mi mujer no es tonta. Sabía que la estaban manipulando. Se disculpó y vino a buscarme.

Prosiguió con su charla cargando las tintas en la escasez de su producto. Esta situación puede servir como lección para no caer en esta trampa. El problema es que hay emociones implicadas. Había visto que tenía una parrilla en el jardín con aspecto de utilizarse a menudo, así que sabía que nos gustaba preparar barbacoas en el jardín y utilizó esa información. Después habló de la calidad de la carne y la comparó con la que normalmente se encuentra en los restaurantes.

Esta táctica de ventas habría funcionado con mucha gente. "¿Y si es la última caja de verdad?". "Es verdad, sale más barato que comer fuera". "Viene hasta casa, no tengo que ir hasta la tienda". Sin embargo, saqué una calculadora y le pregunté el precio de las dos últimas cajas, lo dividí por el peso y le pregunté a mi mujer a cuánto pagaba el kilo de chuletón o de entrecot en la tienda. Cuando descubrimos que ella pagaba 3 euros menos por kilo, permanecí en silencio. Ahora sus emociones entraban en juego. Intentó no quedar en evidencia e inmediatamente bajó su precio en 150 euros. Volví a hacer los cálculos y todavía cobraba el kilo 50 céntimos más caro.

Comenzó a explicar que la calidad de la carne compensaba que fuera 50 céntimos más cara. Cambié mi postura y mi posición alejándome de él para poder mostrar desinterés. Me mantuve en silencio hasta que cortó su charla y me ofreció otra rebaja de 50 euros. Le dije: "Lo siento, pero creo que sigue sin merecer la pena".

Entonces cometió el clásico error que demuestra que el argumento de la escasez de su producto era falso: se derrumbó un poco más. "¿Cuánto quiere pagar por estas dos cajas?".

"Creo que 100 euros estaría bien".

"Si me da 125 euros tenemos un trato".

Recuerde que hacía sólo un momento estaba pidiendo 400 euros por cada caja y eran las últimas que iba a haber por aquí hasta dentro de dos o tres meses. Con un producto tan valioso tendría que haberse iniciado una puja pero finalmente se fue con sus dos cajas y sin el dinero.

La lección que se puede aprender aquí es que para que la escasez funcione tiene que ser real o tiene que mantenerse firme para poder dar la apariencia de que es real.

Cuando algo se necesita realmente la gente le otorga más valor. Un ejemplo mal intencionado es cómo las compañías petrolíferas aumentaron el precio de la gasolina después del huracán *Katrina*. Explicaron que había escasez de petróleo debido al desastre y por eso subieron tanto los precios. Por supuesto, si eso hubiera sido cierto la gasolina costaría todavía mucho más de lo que cuesta; no es más que un ejemplo de cómo utilizar la excusa de la escasez para ganar más dinero. Por otro lado, cuando el terrible error de BP provocó que millones de litros de crudo se perdieran en el Golfo de Méjico destrozando el ecosistema, el precio de la gasolina bajó, en lugar de dispararse, debido a la escasez. ¿Cómo es posible? Bueno, no voy a entrar en eso ahora, pero demuestra que para que la escasez funcione, tiene que ser creíble y ése fue el error de las compañías petrolíferas.

Desde el punto de vista de la ingeniería social, cuanto más limitada o difícil de conseguir sea una oportunidad, más valor tendrá para la gente. Si tiene una información restringida, privada o de difícil acceso y está deseando compartirla con alguien, acaba de aumentar su valor a los ojos de esa persona.

Un auditor de seguridad puede maximizar el efecto de la escasez de la información con una afirmación como "no debería decir esto, pero..." o "no sé si se ha enterado por las noticias, pero he oído...". Afirmaciones como éstas, realizadas en un tono confidencial, potencian el sentido de escasez de esa información.

Autoridad

La gente está más dispuesta a seguir las recomendaciones o direcciones de las personas que ven como una autoridad. Es muy poco habitual encontrar a una persona con la suficiente seguridad en sí misma como para cuestionar directamente la autoridad, especialmente cuando esa autoridad tiene un poder directo sobre ella o está cara a cara con ella.

A los niños, por ejemplo, se les educa para que obedezcan a adultos como los profesores, los curas y las niñeras porque tienen autoridad sobre ellos. A menudo, cuestionar la autoridad se considera una falta de respeto y la obediencia se recompensa. Estos principios se mantienen hasta la edad adulta porque se nos educa para respetar a la autoridad y a no cuestionar las normas o las órdenes que provienen de las personas que consideramos autoridades.

Desgraciadamente, este principio es uno de los motivos por lo que los niños caen en manos de abusadores. Estas personas saben cómo se educa a los niños respecto a la autoridad y normalmente buscan a los que parecen más obedientes. De modo parecido, los ingenieros sociales maliciosos utilizan este principio para manipular a sus objetivos para que realicen una acción que pueda conducir a una brecha de seguridad.

Es importante comprender cómo se emplea la autoridad en el ámbito de la seguridad. El sociólogo y economista político Max Weber definió la autoridad en categorías que he adaptado para que se ajusten al campo de la ingeniería social.

La autoridad legal

La "autoridad legal" se basa en el gobierno y en la ley. Esto se aplica normalmente a los agentes de las fuerzas del orden del territorio donde se encuentre.

Como ingeniero social, crear pretextos que impliquen a agentes del orden u otros oficiales gubernamentales suele ser ilegal. No obstante, se puede representar el papel de guardias de seguridad, vigilantes jurados, etc.

En un episodio de la serie de televisión de la BBC *The Real Hustle*, Paul Wilson y sus ayudantes se disfrazaron de guardias de seguridad para recolectar dinero. Cuando alguien va vestido y se comporta de la misma manera en que una persona en esa posición autoritaria lo haría, los objetivos no tienen ninguna razón para dudar que esa persona sea quien dice ser. Actuar en el papel de una persona con autoridad es una gran estrategia para lograr acceder a una empresa.

Orta estrategia efectiva es representar el papel de un abogado que necesita cierta información. Una manera de emplear la estrategia de una autoridad legal es representando el papel de alguien que la gente suele temer o respetar.

La autoridad de la organización

La autoridad de la organización es sencillamente cualquier autoridad dentro de una organización concreta. Normalmente, el término se refiere a la jerarquía de supervisión de una empresa. Alguien que esté en una posición de poder en una organización tiene acceso a más información que alguien en la parte baja de la jerarquía.

En una auditoría de seguridad, se puede representar el rol de un director general o alguien con una autoridad similar. El auditor puede obtener contraseñas y otros datos del servicio de soporte técnico o de cualquier empleado que perciba que el personaje representado tiene más autoridad que él.

En un artículo titulado "The 'Social Engineering' of the Internet Fraud" (La "ingeniería social" del fraude en Internet), Jonathan J. Rusch del Departamento de Justicia de Estados Unidos escribió: "La gente, en la situación adecuada, es altamente propensa a ser muy receptiva con las demostraciones de autoridad, incluso cuando la persona que pretende estar en la posición de autoridad no está presente físicamente" (`www.isoc.org/inet99/proceedings/3g/3g_2.htm`).

Otra forma de emplear esta estrategia es, en lugar de actuar como un director general, actuar como alguien enviado por el director general. La autoridad que emana el nombre y el título puede ser suficiente para otorgar poder al atacante a ojos del objetivo.

Rusch cita un experimento desarrollado por Robert B. Cialdini y recogido en su libro *Influir en los demás* de 1993, en el que el 95 por 100 de enfermeras de distintos centros de tres hospitales diferentes estaban dispuestas a administrar a los pacientes una dosis peligrosa de medicación basándose exclusivamente en la llamada de un supuesto investigador que las enfermeras no conocían.

Este experimento demuestra claramente que, basándose en órdenes y en la percepción de autoridad, la gente lleva a cabo acciones que pueden ir en contra de su propio juicio. Este tipo de método se utiliza a menudo para conseguir que las empresas revelen información valiosa.

Autoridad social

La autoridad social se refiere a los "líderes naturales" de cualquier grupo social. Un grupo social puede estar compuesto por compañeros de trabajo, amigos o cualquier otra unión de personas.

En *Influir en los demás*, Cialdini escribe: "Cuando se reacciona ante la autoridad de forma automática, normalmente se hace en respuesta a los símbolos de autoridad en lugar de su sustancia".

La autoridad social no necesita una gran estructura ni demasiado tiempo para ejecutarse. En cualquier situación, un rápido destello de "prueba social", por la que la gente se ve influenciada por un grupo de gente llevando a cabo la misma acción, puede ser suficiente para otorgar autoridad social a una persona.

La autoridad social se puede aprovechar para presionar al objetivo para que revele información. Si el objetivo rehúsa, defraudando al líder, puede perder el favor de todo el grupo. Sin embargo, satisfacer al líder es percibido como algo ventajoso.

La autoridad social se emplea con éxito cuando se afirma directa o implícitamente que otra persona o grupo ha reaccionado previamente del modo que el atacante está solicitando. "Ayer me llamó el director general para solucionar su problema y Joe comprobó mis credenciales y me dejó pasar. ¿Guardó mis datos en el ordenador?". Una afirmación sencilla como ésta utiliza varias formas de autoridad.

Si accede a las peticiones de la autoridad sin pensarlo, puede que esté respondiendo a los "símbolos de autoridad" más que a la realidad. En los países occidentales, existen tres símbolos de autoridad especialmente efectivos. Presentando cualquiera de ellos, la gente estará conforme sin requerir ninguna otra evidencia de autoridad:

- Títulos.
- Vestimenta.
- Automóviles.

En una entrevista que realicé a la doctora Ellen Langer, la psicóloga de Harvard especializada en la persuasión y la influencia (`www.social-enginerr.rog/episode-007-using-persuasion-on-the-mindless-masses`), habló abundantemente sobre la obediencia ciega. Afirmó que la mayoría de la gente suele realizar su trabajo en un estado en el que no necesita pensar demasiado; en otras palabras, funciona con el piloto automático.

En tal situación, el abuso del papel de la autoridad es muy peligroso. La percepción de la autoridad puede hacer que alguien con el piloto automático reaccione sin límite.

Utilizar la vestimenta adecuada, el lenguaje corporal o una tarjeta de visita falsa funciona para representar una posición autoritaria y mantener al objetivo con el piloto automático.

Pueden utilizarse otras formas de autoridad pero las explicadas aquí son las que se utilizan más a menudo. La autoridad es una fuerza poderosa a la hora de influenciar a los demás y, con un poco de razonamiento y de recopilación de información, un ingeniero social puede utilizar un pretexto de autoridad de forma muy efectiva.

Compromiso y coherencia

La gente valora la coherencia en los demás y también intenta mostrase coherente en su propia conducta. Normalmente, la gente quiere que sus palabras, actitudes y hechos resulten coherentes y congruentes. La coherencia reduce la necesidad de procesar la información y ofrece atajos hacia decisiones importantes.

La intuición (esos momentos en los que siente que una acción es buena o mala o correcta o incorrecta, basándose en experiencias pasadas) suele ser indicadora de que la decisión que se está tomando puede ir en contra de sentimientos y creencias previamente existentes. Estas señales indican normalmente que se está viendo empujado a aceptar algo que no quiere en realidad.

La intuición también puede aparecer a la hora de comprometerse. En ese caso, puede indicar que no está seguro de que ese compromiso no sea un error. Puede preguntarse a sí mismo: "Sabiendo lo que ahora sé, si pudiera hacerlo otra vez, ¿volvería a comprometerme a algo así?".

Antes de explicar cómo puede utilizar un ingeniero social la coherencia para lograr el compromiso de otra persona, veamos unos ejemplos que ayudarán a comprender esta idea.

- **Marketing:** Normalmente, las empresas gastan cantidades extraordinarias de dinero en ganar su cuota de mercado. No hay un retorno real de la inversión pero, aun así, luchan por mantener esa cuota que consideran rentable. Coca-Cola y Pepsi son dos buenos ejemplos de empresas que han utilizado el marketing durante décadas en un esfuerzo por mantenerse visibles, a pesar de que en muchas ocasiones sus anuncios no pretenden influenciar a la gente para que cambie de Pepsi a Coca-Cola. Debido a que las dos empresas se muestran "comprometidas" a la guerra la una contra la otra, parece que cuando una de ellas presenta un nuevo producto o idea la otra no puede ir muy a la zaga.
- **Subastas:** La popularidad creciente de las casas de subastas *on-line* como eBay muestran con claridad este principio. La gente siente cierto compromiso hacia aquello sobre lo que ha pujado y, si alguien sobrepuja, se siente obligado a pujar de nuevo. En ocasiones, aumentan sus pujas mucho más allá de lo que consideran razonable simplemente porque se sienten obligados. Un ejemplo clásico de esto es cuando Robert Campeau compró Bloomingdales. Pagó 600 millones de euros por encima del precio estimado. Max Bazerman, autor de *La negociación racional: en un mundo racional* citó a un periodista de Wall Street Journal diciendo: "Ya no es una cuestión de precios sino de egos...".
- **Ferias, casas de juego, etc.:** Siempre que haya casas de apuestas o de juego implicadas existe un gran riesgo de que se utilice la coherencia y el compromiso para persuadir a la gente. El columnista Ryan Healy, un consultor de marketing *on-line*, escribió una historia sobre un día en que llevó a su hija a un circo (`www.ryanhealy.com/commitment-and-consistency/`). Gastó 44 euros en las entradas, 5 euros en el aparcamiento

y empleó un total de 40 minutos de coche en ir y volver. Estaba obligado a estar en el circo. Su hija quería algodón de azúcar y accedió entregándole 5 euros. ¿Puede costar más de eso el algodón de azúcar? Cuando le dijeron que costaba 12 euros, ¿cómo podía echarse atrás en su compromiso con su hija? No podía y, por tanto, acabó gastando 12 euros en un algodón de azúcar.

La coherencia se define en este ámbito como lo que se espera en base a experiencias o expectativas previas. La experiencia o expectativa puede motivar que el objetivo realice una acción que provoque una brecha. Por ejemplo, cuando llega el técnico de asistencia, se espera que entre en el cuarto del servidor. Esa petición es coherente con las expectativas y experiencias previas. Cuando se solicita el acceso al cuarto del servidor es más probable que se conceda porque es coherente con lo que se espera.

El compromiso y la coherencia pueden ser importantes factores de influencia para que mucha gente realice acciones, revele información o divulgue algún secreto.

Un ingeniero social puede hacer del compromiso y la coherencia unas de sus mejores armas. Si consigue que un objetivo se comprometa a realizar alguna acción pequeña, normalmente no es difícil ampliar ese compromiso hacia cotas más altas.

En su libro *Influir en los demás*, Robert Cialdini escribe:

La clave para utilizar los principios del compromiso y la consistencia para manipular a la gente se encuentran en el compromiso inicial. Esto es: después de comprometerse, tomar una postura o posición determinada, la gente estará más dispuesta a acceder a peticiones que sean coherentes con el compromiso previo. Quienes emplean estos métodos intentan persuadir a otros para tomar una posición inicial concreta que sea coherente con una conducta que solicitarán más adelante.

Un ingeniero social que quiera emplear la técnica del compromiso y la coherencia normalmente intentará que el objetivo revele una información poco importante pero que vaya encaminada hacia la meta final. Al lograr que el objetivo mantenga la coherencia en las cosas que dice o hace, el atacante conseguirá que el objetivo revele más información.

Por otro lado, el atacante también debe mantener la coherencia en lo que pide. Debe realizar la recopilación de datos empezando por elementos menores para ir pasando a información cada vez más importante.

Utilizando un ejemplo irreal, el atacante nunca debe empezar pidiendo los códigos de un lanzamiento nuclear. Esta petición será denegada y al atacante le quedarán pocas opciones, aparte de dar marcha atrás. Sin embargo, empezando

por elementos pequeños y aumentando poco a poco el valor de la información solicitada, creará una progresión que resultará más natural y que no parecerá tan obvia para el objetivo. Ir despacio y en progresión puede ser difícil porque los ingenieros sociales suelen ser impacientes y quieren conseguir la "contraseña" inmediatamente. Pero tomárselo con calma y ser paciente tiene su recompensa. Definir, incluso escribir, el camino a seguir le ayudará a comenzar la auditoría con metas perfectamente definidas y el modo de alcanzarlas. He creado un gráfico que puede ver en la figura 6.2 que muestra cómo puede visualizarse este camino para obtener información utilizando el compromiso y la coherencia.

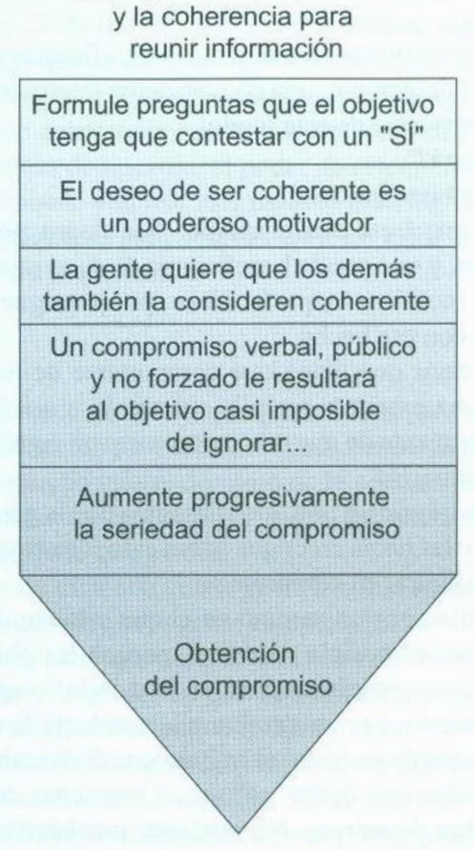


Figura 6.2. *Definir claramente sus metas puede ayudarle a lograr un compromiso.*

Si consigue que un objetivo se comprometa verbalmente a realizar cierta acción podrá forzarle por un camino determinado. Cialdini afirma: "La regla del compromiso y la coherencia establece que, una vez que tomamos una decisión,

experimentaremos presión por parte de los demás y de nosotros mismos para comportarnos coherentemente respecto a esa decisión. Puede ser presionado para tomar decisiones buenas o malas dependiendo de acciones pasadas".

Puede que haya sentido algo parecido cuando le dijo a su pareja que iba a perder peso. Ese "compromiso" verbal conlleva mucha presión para mantener el trato hasta el final.

En ocasiones, acabar discrepando con uno mismo puede resultar muy difícil, si no imposible. Todo el mundo en algún momento de su vida ha murmurado la frase: "Lo siento, he cambiado de idea". Cuando lo hacemos, nuestra cabeza se inclina por la vergüenza, nuestro tono de voz cae y sonamos muy tristes. ¿Por qué? Acabamos de romper nuestro compromiso y nos sentimos muy culpables por ello.

Incluso los compromisos aparentemente insignificantes pueden conducir a una brecha importante. Por ejemplo, una conversación telefónica empleada a menudo por los abogados transcurre de este modo:

"Hola, ¿qué tal está?".

Responde: "Muy bien, gracias".

A continuación, prepárese para el ataque: "Me alegro, porque hay gente que no se encuentra tan bien y que puede beneficiarse de su ayuda".

Ahora no puede rectificar lo que ha dicho, porque sigue encontrándose bien y está comprometido con ese hecho.

Esto no quiere decir que tenga que comportarse de manera paranoica y no pueda contestar a una pregunta sencilla sin miedo a que le manipulen, pero es fundamental ser consciente de que un compromiso no significa que deba comprometerse más a continuación.

Hace tiempo trabajé con un tipo que conseguía que la gente hiciera literalmente los peores trabajos y les hacía creer que había sido idea suya. Uno de los métodos que empleaba era asegurar su compromiso.

Si se comprometían por un camino en el que estaban de acuerdo con ciertas cosas, lo que era casi imposible de evitar, porque les obligaba a decir "sí" de antemano, entonces continuaban accediendo a todo lo que les pedía después. Continuaban accediendo, por un camino que conducía hacia donde él quería, a que estuvieran de acuerdo en hacer el trabajo que él deseaba.

Es importante saber que decir "no" en un momento dado puede salvarle de comprometerse a algo desastroso. No obstante, muchas veces nos convencemos a nosotros mismos de que decir "no" es una especie de pecado capital que sólo se nos perdonará rezando mucho.

En el ejemplo anterior del vendedor de carne, mi mujer es una persona muy consciente de sí misma. Sabía que podía ser manipulada por un "aparente buen trato", así que entró a buscarme porque sabe que soy un "tarado".

Uno de los mejores ejemplos que conozco sobre el poder del compromiso es un experimento social realizado por el doctor Thomas Moriarty en 1972. Mandó a un ayudante a la playa como "víctima" con una radio portátil. Se sentó en la silla a escuchar la radio durante diez minutos y después se levantó para ir a comprar un refresco.

En ese momento, otro ayudante, el "ladrón", apareció para "robar" la radio. Sólo 4 de un total de 20 personas (sólo el 20 por 100) intentaron evitar que el ladrón robara la radio.

Entonces los investigadores subieron la apuesta con un nuevo intento. Antes de que la "víctima" se levantara a por la bebida le pediría a una de las personas de alrededor que vigilara la radio. ¿Cuál cree que fue el resultado?

Sorprendentemente, 19 de los 20 detuvieron al ladrón, algunos incluso recurriendo a la violencia. ¿A qué se debe esta asombrosa diferencia? Al compromiso y la coherencia. El investigador logró un compromiso de los vecinos de la víctima y eso les hizo actuar con coherencia respecto a ese compromiso. En mi opinión, estas increíbles estadísticas demuestran el poder de este método de influencia.

Un ingeniero social puede emplear este método para lograr que el objetivo se comprometa acciones pequeñas para después emplear ese compromiso para progresar hacia acciones más importantes.

Agradar

A las personas les gusta la gente a la que gustan. Aunque esta frase parezca un trabalenguas, es una afirmación muy cierta. Al comprender la profundidad de esta afirmación se acercará mucho más al dominio de la persuasión.

Cuando digo "comprender la profundidad" me refiero exactamente a eso, porque esta frase es mucho más de lo que parece.

Esta afirmación no está diciendo que la gente a la que agrade responderá bien. A los vendedores se les enseña que la gente compra a las personas que le agradan. Esto es cierto, pero no es exactamente a lo que nos referimos. Tampoco está diciendo que debe agradar a la gente. Lo que está afirmando es que a usted deben gustarle las personas y a cambio usted les gustará a ellas.

Esta tarea no es tan fácil como parece porque no se puede fingir que alguien nos guste. Como explicamos en el capítulo 5, las sonrisas y la felicidad son muy difíciles de fingir. Debe abordar las acciones preocupándose realmente por las personas a las que está intentando influenciar. Los ingenieros sociales maliciosos no se preocupan por la gente y sus sentimientos, por lo que sustituyen esta práctica por el encanto personal. El encanto puede funcionar a corto plazo, pero a largo plazo es necesario desarrollar la habilidad de que las personas le gusten de verdad.

Este principio se utiliza habitualmente en el campo del marketing. En 1990, Jonathan Frezen y Harry Davis publicaron un estudio titulado "Purchasing Behavior in Embedded Markets" (Hábitos de compra en mercados integrados) que examinaba por qué las "reuniones Tupperware" eran tan exitosas (`www.jstor.org/pss/2626820`). Toda su investigación condujo a este principio de agradar a los demás.

Los investigadores concluyeron que mucha gente compraba en estas reuniones porque quería que el anfitrión se sintiera bien, para ayudar a un amigo o para agradar a los demás. ¡Qué embarazoso sería acudir a una de estas reuniones y no comprar nada! Ese miedo a no agradar es lo que empuja a la mayoría de la gente a comprar y no tiene nada que ver con necesitar un Tupperware más.

Otros informes y estudios han comprobado la confianza que la gente tiene en un consejo dado por quienes consideran sus amigos y la confianza que tienen en personas desconocidas o incluso personas que no les gustan. Una persona está más dispuesta a seguir un mal consejo de un amigo que un buen consejo de alguien que le disgusta.

Para un auditor de seguridad este concepto es una herramienta efectiva. No sólo debe agradar y ganarse la confianza de las personas, debe estar verdaderamente interesado en ellas. Este concepto vuelve al tema del pretexto explicado en el capítulo 4. Cuando desarrolla un pretexto no está simplemente actuando, debe convertirse en la persona que representa; ese papel es su vida. Si lo consigue, el paso de que le guste la gente será más sencillo. Su pretexto estará realmente interesado en ayudar y agradar a esa persona.

Orto aspecto importante de este principio es el atractivo físico. Los seres humanos tendemos a que nos "guste" automáticamente la gente que consideramos atractiva. Por muy superficial que suene, es la verdad. Algunos principios psicológicos muy serios apoyan esta idea.

Lo hermoso es bueno. En 1972 Berscheid, Walster y Dion elaboraron un estudio titulado precisamente así, "What Is Beautyful Is Good" (Lo hermoso es bueno), que hizo descubrimientos importantes. Se pidió a los participantes que clasificaran las fotos de tres individuos en un rango de atractivo alto, medio y bajo. Basándose en esas fotos solamente, debían clasificarlos por su carácter, su felicidad y su éxito profesional

Después, se recopilaron las puntuaciones y descubrieron que las personas consideradas más atractivas eran las más deseadas socialmente, tenían mejores ocupaciones, eran más felices y más exitosas. El estudio demostró que la gente tiende a relacionar la belleza con otras cualidades positivas y altera sus opiniones y su capacidad para confiar en una persona.

Este estudio es un ejemplo del fenómeno conocido como "efecto halo", en el que un rasgo particular de la persona afecta o se extiende a otras de sus cualidades. Se ha demostrado que afecta a las decisiones de una persona con una tendencia

a centrarse en los rasgos positivos de la otra. He archivado una copia de este asombroso estudio en `www.social-engineer.org/wiki/archives/BlogPosts/BeautifulGood.pdf`.

En otras palabras, si alguien le encuentra atractivo, esa característica se extiende al resto de juicios que esa persona se forme sobre usted. El efecto halo se emplea a menudo en el marketing. Se muestra a gente atractiva bebiendo, comiendo y vistiendo ciertos productos y los consumidores piensan automáticamente "este producto será bueno si lo utiliza esta gente tan atractiva".

Recientemente, vi un anuncio en televisión que ilustraba esta idea con claridad. El anuncio se reía de las tácticas del marketing, pero lo hacía de un modo muy inteligente. Aparecía en pantalla una chica guapa vistiendo ropa atractiva que decía: "Hola, soy una chica de entre 18 y 24 años considerablemente atractiva".

Utilizar una chica agradable, no atractiva en exceso pero claramente real, alguien a quienes las personas normales podamos admirar, es una jugada de marketing genial. No podemos concretar su edad pero es cierto que la podemos situar en algún punto entre los 18 y los 24 años.

"Te puedes relacionar conmigo porque soy racialmente ambigua".

De nuevo, un punto genial. No es exactamente blanca, ni negra, ni oriental. No lo podemos saber, puede ser una mezcla que resulte atractiva para cualquier raza y que no sea ofensiva para casi nadie.

"Estoy en este anuncio porque las investigaciones de marketing indican que a las chicas como tú le gustan las chicas como yo".

Su belleza y su confianza en sí misma hacen que nos guste; viste bien, habla correctamente y nos gustaría conocerla.

Entonces se muestran distintas imágenes de la chica haciendo cosas como practicar *kickboxing*, hacer de animadora y jugar con flores. Al mostrarla a los espectadores haciendo estas cosas, unido a lo guapa que es, la consideramos fuerte y poderosa y percibimos como positivo todo lo que hace. "Ahora voy a decirte que compres algo...".

Entonces pasa a vender una marca de tampones. Este anuncio es genial porque se subrayan y emplean los métodos que hacen que el consumidor quiera comprar. Pero, sobre todo, en este anuncio descansan los principios de agradar y el efecto halo.

Sabiendo la importancia de este principio, ¿qué puede hacer? Puede resultarme extremadamente difícil pasar por un hombre atractivo, no digamos por una mujer. Como las visitas al cirujano plástico quedan descartadas, ¿qué puede hacer un ingeniero social para aprovechar este principio?

Conozca a su objetivo. Infórmese sobre lo que le resulta aceptable e inaceptable. ¿Cómo viste y qué considera bueno y malo? Demasiado maquillaje o demasiadas joyas pueden provocar rechazo en el objetivo. Imagine que quiere auditar la con-

sulta de un médico y su pretexto es un representante de un laboratorio. Sabe que la mayoría de representantes visten traje; llevan el cabello perfecto; tienen buen aspecto, huelen bien y actúan con confianza, un rasgo común de la gente atractiva, por lo tanto, aparecer con el pelo de punta y *piercings* en la cara hará que llame demasiado la atención.

Debe conocer a su objetivo para presentarse con el aspecto que él espera. Lleve ropa, peinados, maquillaje y complementos que no sorprendan, choquen o disgusten al objetivo. Haga que se sienta cómodo creando un entorno que favorezca que pueda gustarle, lo que generará confianza y le conducirá al éxito.

Puede buscar cosas con las que halagarlo. Cuando sea adecuado, empiece la conversación con una sencilla pregunta halagadora como "esos zapatos son bonitos, ¿dónde los ha comprado?". A la gente le gusta el refuerzo positivo. Cuando la gente recibe halagos de otra persona tiende a mantenerse atento para recibir más refuerzo positivo. Estos halagos consiguen reforzar la autoestima del objetivo, haciéndole sentir que le conoce de forma especial.

La Universidad de Minnesota presentó un artículo (`www.cehd.umn.edu/ceed/Publications/tipsheets/preschoolbehaviortipsheets/posrein.pdf`) sobre el refuerzo que afirma que un exceso de refuerzo positivo puede ser contraproducente. Lo llaman saciedad y significa que, cuando se abusa de los refuerzos, empiezan a perder efecto. Para contrarrestar este efecto, puede respaldar los refuerzos positivos con una pregunta. Este método refuerza las conductas y actitudes positivas y también hace feliz a la gente cuando se le pregunta por sí misma.

Estos cuatro pasos pueden lograr que le guste a la gente:

1. Proyecte una actitud confiada y positiva.
2. Establezca una compenetración.
3. Sintonice con el objetivo y su entorno utilizando los métodos explicados anteriormente.
4. Comunique con eficacia.

En su libro *Cómo caer bien a los demás en menos de 90 segundos: aprende a leer el lenguaje corporal y a establecer conexiones cálidas y llenas de significado*, Nicholas Boothman afirma que la gente decide si le gusta una persona a los dos segundos de conocerla. Después de que se forme una impresión, es difícil cambiarla. Él sugiere entrar en una interacción con una buena actitud. Tener la habilidad de comunicarse de forma efectiva en situaciones diferentes puede hacerle más atractivo a los ojos del objetivo. Lo que proyecta sobre los demás es lo que ellos perciben. Sus expresiones faciales, el lenguaje corporal y la vestimenta deben proyectar una actitud positiva.

Boothman explica puntos fundamentales en su libro, como la necesidad de hacer muchas preguntas, escuchar activamente y mostrarse muy interesado en todo lo que la gente dice. Puede que necesite practicar, pero conseguir gustar a los demás le ayudará mucho en sus auditorías de seguridad.

El consenso o prueba social

La prueba social es un fenómeno que tiene lugar en situaciones sociales en los que la gente no es capaz de determinar cuál es el modo adecuado de comportarse. Puede asumir fácilmente cuál es la conducta adecuada si ve a otros comportarse de esa manera. La influencia social en general puede conducir a grandes grupos de individuos a estar conforme en tomar opciones correctas o equivocadas. Esta conducta es común cuando se entra en una situación poco familiar y no se tiene un marco de referencia sobre cómo comportarse; imitan la conducta de quienes consideran que están más familiarizados con la situación y, por tanto, mejor informados.

En su libro *Influir en los demás*, el doctor Robert Cialdini afirma: "La prueba social: la gente hará las cosas que ve hacer a los demás. Por ejemplo, en un experimento, uno o dos cómplices mirarán al cielo; la gente de alrededor mirará al cielo también para comprobar qué están mirando. Este experimento tuvo que detenerse en cierto punto porque había tanta gente mirando al cielo que bloqueó el tráfico".

Señalaré algunos buenos ejemplos de prueba social que le ayudarán a comprobar lo poderosa que es y si alguna vez ha caído en ella. La prueba social se emplea mucho en marketing. Se utiliza cuando se publican cifras de ventas abultadas, demostrando a los clientes potenciales que el producto es muy popular.

Otro ejemplo se da cuando las empresas distribuyen camisas con logos impresos para que, quienes las lleven puestas, realicen una promoción implícita.

La prueba social no sólo influencia a través de grandes grupos de personas, sino también a través de personajes destacados. Por ejemplo, al asociar a una celebridad con un producto se consigue que la gente quiera asociarse con los rasgos positivos de esa personalidad y utilizarán ese mismo producto.

Existen muchos ejemplos de la utilización de personajes famosos para realizar promociones publicitarias, aquí puede ver algunos:

- Un importante fabricante de gorras logró que Samuel L. Jackson promocionara su producto, la gorra Kangol.
- Durante el año 2010, Maria Sharapova cobró millones de euros por promocionar productos Canon.

- Catherine Zeta Jones promociona productos T-Mobile en anuncios de televisión y vallas publicitarias por la friolera de 20 millones de euros.
- En 2009, Tiger Woods cobró más de 100 millones de euros de AT&T, Gatorade, Gillette, Niké, Golf y TAG HEUER, por nombrar algunos.
- Michael Jordan sigue ganando 45 millones de euros al año por sus anuncios para Nike.
- Ozzy Osbourne promociona una marca de margarina.
- Mikhail Gorbachev publicita Louis Vuitton.
- Ben Stiller promociona la bebida Chu High para el público japonés.

¿Por qué las empresas gastan tanto dinero en que un famoso promocione sus productos? Así es exactamente como funciona la prueba social. Cuando los consumidores ven a la gente famosa que admiran y adoran vistiendo, utilizando o hablando sobre estos productos, sienten como si esa persona les estuviera diciendo directamente a ellos lo estupendo que es ese producto. Muchos interpretarán esto como la prueba de que merece la pena gastar el dinero en ese producto

En sus comunicaciones publicitarias, la empresa afirmaba que sus gorras eran las más atractivas del mercado y la prueba estaba en que el señor Jackson las llevaba.

Los publicistas a menudo utilizan expresiones como "líder de ventas" o "el producto de moda", para convencer a su audiencia de que tienen el apoyo de muchos de nuestros semejantes en sus afirmaciones.

Además, el sitio Web de Media-Studies.ca publicó un artículo sobre la influencia de los objetivos utilizando la prueba social (`www.media-studies.ca/articles/influence_ch4.htm`):

Los experimentos han demostrado que el uso de risas enlatadas provoca que la audiencia ría por más tiempo y más a menudo cuando se les presenta material humorístico y hace que consideren ese material más gracioso. Además, existen evidencias de que las risas enlatadas son más efectivas en el caso de los chistes malos. La cuestión es: ¿por qué funciona, sobre todo teniendo en cuenta que en la mayoría de los casos es muy evidente que la risa es falsa? Para responder a esta pregunta, Cialdini propone el principio de la prueba social: "Un modo que utilizamos para determinar qué es lo correcto es descubrir lo que otros consideran que es correcto... Consideramos una conducta más correcta en una situación determinada en el grado en que vemos a otros realizándola".

Al igual que con las demás "armas de influencia", la prueba social es una vía que suele funcionar muy bien para nosotros: si nos adaptamos al comportamiento que vemos a nuestro alrededor, es más probable que evitemos meter la pata. El

hecho de que las risas enlatadas provoquen una respuesta automática de la audiencia sugiere que las pistas auditivas son un poderoso estímulo porque nos impulsan a un nivel de consciencia que nos resulta difícil criticar.

Otro ejemplo es cómo los camareros ponen el bote en un lugar visible y lleno de dinero. Cuando alguien se acerca a la barra el mensaje que recibe es: "Mucha gente ha dejado propina, ¿por qué no lo haces tú también?". ¡Y funciona!

Una de las investigaciones más reveladoras en este campo la llevó a cabo el doctor K. D. Craig en 1978. El doctor Craig dedicó su vida al estudio del dolor y a su efecto en las personas. En 1978, publicó un artículo titulado "Social Modeling Influences on Sensory Decision Theory and Psychophysiological Indexes of Pain" (Modelos de influencia social en la teoría de las decisiones sensoriales e índices psicofisiológicos de dolor) que puede encontrarse en `www.ncbi.nlm.nih.gov/pubmed/690805?dopt=Abstract`, en el que realizó un experimento que describió como:

Los sujetos expuestos a modelos sociales simulando tolerancia o intolerancia normalmente mostraron una conducta paralela en sus evaluaciones verbales de la estimulación dolorosa. No obstante, no queda claro si estos cambios reflejan una alteración voluntaria de las evidencias o cambios reales en la aflicción.

Este estudio emplea medidas alternativas y controladas para la limitación metodológica de estudios previos examinando el potencial de piel no palmar, además de la conductancia de la piel palmar y los índices de ritmo cardiaco de respuesta psico-fisiológica a las descargas eléctricas, y evaluando expresiones verbales de dolor con la metodología de la teoría de la decisión sensorial.

Varios índices de potencial de piel no palmar y de reactividad del ritmo cardiaco mostraron una reactividad más baja en el grupo tolerante. La tolerancia también se asoció con disminuciones en el estrés subjetivo. Los resultados fueron consistentes con el hecho de que los cambios en los índices de dolor asociados con la exposición a un modelo tolerante representaron variaciones en características fundamentales de experiencias dolorosas en oposición a la supresión de información.

Para resumir esto, lo que hizo básicamente el doctor Craig fue someter a descargas eléctricas a un grupo de personas para después pedirle que evaluaran el nivel de dolor. Después, utilizando descargas parecidas hizo la misma prueba pero en presencia de una persona que se mostraba "tolerante" al dolor; asombrosamente, el sujeto también era ahora más tolerante.

Este experimento demuestra que parte de la motivación para exhibir o sentir dolor está relacionada con el modo en que actúan las personas de alrededor. Los sujetos del estudio no actuaban como si les doliera menos: las reacciones en su

piel y el ritmo cardiaco mostraron menos evidencias de dolor cuando estaba presente el modelo tolerante al dolor. Para ver un ejemplo humorístico del poder de la prueba social, eche un vistazo a un vídeo de un antiguo programa de televisión llamado *Candid Camera* en `www.social-engineer.org/framework/Influence_Tactics:_Consensus_or_Social_Proof`.

El vídeo muestra a unos sujetos siendo influenciados para colocarse mirando hacia distintos lados dentro de un ascensor. Incluso llegan a verse influenciados a mirar hacia la parte de atrás simplemente porque el resto de personas lo está haciendo. Hay tres o cuatro cómplices dentro del ascensor que, de forma coordinada van girando hacia la derecha, hacia la izquierda o hacia atrás. En pocos segundos, el sujeto se une y gira hacia el mismo lado, se quita el sombrero como todos los demás o realiza alguna otra acción.

La prueba social es una herramienta muy eficaz. Puede emplearse para estimular la conformidad de una persona a una petición informándola de que muchas otras personas, incluso algunas que pueda considerar como modelos a seguir, han realizado la misma acción que ahora se le pide que realice.

La prueba social puede ofrecer una vía para determinar cómo comportarse y, al mismo tiempo, puede hacer a los objetivos vulnerables a manipulaciones para influenciarlos.

La prueba social resulta más efectiva bajo dos condiciones:

- **Incertidumbre:** Cuando la gente no se siente segura y la situación es ambigua es más probable que observen la conducta de otros y que la acepten como válida.
- **Similitud:** Las personas se sienten más inclinadas a seguir a quienes se parecen a ellas.

En estas condiciones, es cuando un ingeniero social puede utilizar la prueba social. Afirmar o incluso insinuar que mucha gente antes que el objetivo ha realizado cierta acción aumenta las probabilidades de éxito.

En cierta auditoría que estaba llevando a cabo, me paró un guardia de seguridad receloso. Actué como si me sorprendiera que me parase y dije: "Ayer Jim me dejó pasar después de comprobar mis credenciales, suponía que las había registrado".

El guardia, al escuchar que Jim había dado el visto bueno, me dejó pasar sin dudar. La prueba social no siempre funciona con tanta facilidad, pero es un arma poderosa.

Los principios explicados en esta sección son algunas de las tácticas de persuasión más letales de las que se utilizan hoy en día. Estas tácticas pueden darle literalmente el poder de motivar a la gente y hacerla reaccionar de forma que queden bajo el control del auditor de seguridad.

Recuerde que la influencia y el arte de la persuasión es el proceso de lograr que alguien "quiera" hacer, reaccionar, pensar o creer del modo en que "usted" quiera que lo haga. Crear este tipo de motivación en un objetivo es una fuerza muy poderosa; es como un superpoder del ingeniero social. Estos principios pueden hacer de ese superpoder una realidad, pero sólo siendo consecuente y con mucho trabajo.

¿Qué quiero decir con esto? He comprobado en muchas ocasiones que, después de practicar una habilidad y dominarla, es muy difícil "desconectar". Esto puede sonar atrayente pero lo mejor es ser cauteloso respecto a la persona que se está influenciando. Para arraigar estas habilidades en su personalidad, utilícelas para ayudar a los demás. Por ejemplo, cuando empiece a practicar leyendo microexpresiones y a emplearlas para manipular a un objetivo, la reacción inmediata puede ser pensar que tiene una especie de poder místico que poco más que le permite leer las mentes. Aquí es donde la cautela es pertinente. Practique la técnica y trate de perfeccionarla, pero no crea que lo sabe todo.

Si puede influenciar a alguien para que deje de fumar, para que empiece a entrenar o para que lleve una vida más saludable, aprenderá a recurrir a estas habilidades cuando lo desee y ya no estará lejos de poder emplearlas en sus auditorías.

Muchas de estas habilidades requieren que realmente se interese por los demás y empatice con ellos. Si no posee esta habilidad natural, deberá trabajar duro para dominar estas técnicas. Le animo a que se tome tiempo porque con ellas llegará a ser un gran ingeniero social.

Imagine que puede alterar su pensamiento hasta el punto de que le resulte fácil lograr estas habilidades. Imagine también que puede cambiar el pensamiento de sus objetivos de manera que experimenten lo que usted quiere. Alterar la realidad de aquéllos que le rodean y la suya misma es el tema de la siguiente sección, que seguro que le sorprenderá.

Alterar la realidad: el encuadre

El "encuadre" se ha definido como la información y las experiencias de la vida que alteran nuestra manera de reaccionar a las decisiones que debemos tomar. El encuadre son las experiencias propias y de otras personas que permite que penetren en su mente consciente para alterar la manera en que toma decisiones.

Los supermercados utilizan el encuadre cuando en la etiqueta de un paquete de carne ponen "75 por 100 magro" en lugar de "25 por 100 grasa". Los dos términos indican lo mismo en este caso (en ambos casos se trata de un 25 por 100 de grasa) pero uno suena saludable y es atrayente para el consumidor; por eso, las tiendas utilizan el porcentaje de carne magra en lugar de marcar el contenido graso.

Este ejemplo es muy simple pero ayuda a entender el poder del encuadre. Simplemente presentando los hechos de una forma diferente puede conseguir que parezca bueno algo que normalmente consideraríamos malo.

Las siguientes secciones explican algunas áreas en las que a menudo se utiliza el encuadre, para que se haga una idea de su poder.

Política

El encuadre se utiliza en política desde hace mucho tiempo. Simplemente por el modo en que las campañas o los mensajes se formulan se marca una gran diferencia en la forma en que el público los percibe.

Tome en consideración a George Lakoff, un lingüista cognitivo profesional. En una interesante observación sobre el encuadre en la política, explica cómo la gente percibe de forma diferente la frase "antiterrorismo por imperativo legal" en oposición a la frase "antiterrorismo como guerra". Cuando sucedieron los ataques del 11 de septiembre, Colin Powell explicó que estos ataques debían ser tratados como crímenes. Cuando el público pidió más acciones y políticas más estrictas, el presidente Bush anunció la campaña de "guerra contra el terror".

Otro ejemplo es el programa de Seguridad Social de Estados Unidos. El nombre insinúa que se puede depender de él para asegurarse el bienestar en el futuro.

Y un ejemplo más es la diferencia entre los términos "rescate financiero" y "estímulo económico". El término "rescate" se topó con mucha oposición porque podía evocar la imagen de un rescate a los náufragos de un barco hundido. Pero "estímulo económico" forma la imagen mental de una ayuda a la economía estimulándola. Ambos programas consistían prácticamente en lo mismo, pero simplemente el nombre hizo que el segundo término fuera mejor aceptado.

Judith Butler, profesora de Berkeley y autora del libro aclamado por la crítica, *Marcos de guerra. Las guerras lloradas*, escribió sobre cómo se utiliza el encuadre, especialmente en las culturas occidentales, en lo que se refiere a las agendas políticas y a la guerra. En su libro, explora el retrato que hacen los medios del estado de violencia:

Este retrato ha saturado nuestro entendimiento de la vida humana y ha conducido al abandono y explotación de pueblos enteros, a los que se considera amenazas en lugar de poblaciones vivas necesitadas de protección. Se marca a esta gente como si ya estuviera perdida y estuviera destinada al encarcelamiento, el desempleo y la inanición de forma que es fácilmente descartada. En la retorcida lógica que racionaliza sus muertes, la pérdida de tales poblaciones se considera necesaria para proteger la vida de "los vivos".

Éstos son sólo algunos ejemplos de cómo se utiliza el encuadre en el mundo de la política.

Utilizar el encuadre en el día a día

El término "marco de referencia" se define como un grupo de ideas, condiciones o asunciones que determinan cómo algo debe ser abordado, percibido o comprendido. Esta definición puede ayudar a comprender cómo se utiliza el encuadre.

Cualquier cosa que pueda alterar la percepción de la gente o el modo en que toma decisiones puede denominarse encuadre. Un amigo le cuenta que la semana pasada fue a la ciudad tomando una ruta que tenía 15 kilómetros de atasco debido a unas obras. Puede que la próxima vez usted elija la ruta más larga para evitar el potencial retraso, a pesar de que la información que le dio su amigo es de hace una semana.

Nuestra mente está diseñada para que no le guste el "desorden" o el caos. Cuando afronta cosas que están desordenadas, nuestro cerebro trata de ordenarlas. Un interesante ejemplo de esta idea se puede encontrar en la figura 6.3.

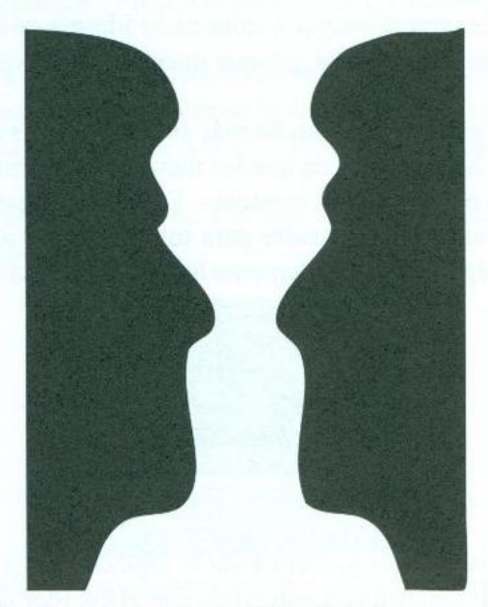


Figura 6.3. *¿Puede alterar su marco de realidad para cambiar lo que ve?*

En nuestro marco actual, ¿qué es el fondo y qué es el primer plano? Su cerebro insistirá en buscar patrones familiares en las cosas. Lo hacemos con las nubes, con el espacio y con los objetos inanimados. También tendemos a ver caras en este tipo de cosas.

En la figura 6.4, ¿puede alterar su encuadre y cambiar lo que es la imagen y lo que es el fondo? Intente centrarse en lo contrario a lo que vio primero.

Otro ejemplo interesante sobre cómo el cerebro humano encuentra orden en el caos se puede ilustrar con un correo electrónico que circuló en los últimos años y que decía así:

Slóo la gtene ltisa pedue leer etso.

No pdueo ceerr que sea cpaaz de ednentr lo que eosty lyendeo. El abosrmsoo peodr de la mtene hmunaa. Sgúen una itagióvniescn riedazala en la Uvsirandied de Cigarbmde, no ioptmra el odern en que etésn las pbaralas, lo úicno que imtrpota es que la pirerma y la úitmla parlaba etésn en el siito certcoo. El rteso peude etasr en cmetolpo ddoeresn y aún así pdroá lreleo sin pemrboals. Etso es ddiboeo a que el creprebo hmuano no lee cdaa ltera por saredpao, snio la pbaarala cmoo un tdoo. ¿Ibcilrene, vraded? ¡Y yo que pnbasea que la ofortígara era irnamtopte! Si pedeus leer etso, ¡plasáo!

No estoy seguro de que sea una investigación de la Universidad de Cambridge, pero lo interesante de este correo electrónico es la cantidad de gente que utiliza el castellano como lengua principal o domina el idioma que es capaz de leer el párrafo sin demasiados problemas, porque nuestros cerebros son muy eficientes ordenando el caos.

Muchas veces el encuadre es mucho más subliminal. Las empresas lo utilizan en el marketing con la esperanza de que los mensajes subliminales alteren la percepción que tiene el objetivo de su producto. En muchas ocasiones, las empresas utilizan cantidades sutiles de encuadre para implantar una idea. Por ejemplo, la figura 6.4 muestra algo que probablemente habrá visto muchas veces.



Figura 6.4. *¿Puede localizar el encuadre?*

Después de ver esto, nunca volverá a ver el logo de FedEx de la misma forma. Hay una flecha en el logo. En una entrevista con el creador del logo, dijo que insertó la flecha para implantar una idea sobre los servicios de FedEx. Está ahí para comunicar movimiento, velocidad y la naturaleza dinámica de la empresa. ¿La ha encontrado ya? Mire la figura 6.5, donde he marcado la flecha y la he rodeado con un círculo.

FedEx no es la única empresa que utiliza el encuadre. Durante décadas, las empresas han estado insertando mensajes en sus logos en un esfuerzo por encuadrar el pensamiento de los consumidores para que recuerden, vean y piensen en la empresa como ellos quieren. Las siguientes figuras muestran algunos ejemplos más.



Figura 6.5. *La flecha indica un servicio de calidad en continuo movimiento.*

¿Alguna vez se había fijado en que el logo de Amazon contiene un mensaje insertado? Vea la figura 6.6.



Figura 6.6. *¿Puede ver el cliente feliz y sonriente?*

Amazon tiene dos mensajes insertados en su logo. Uno es la felicidad que siente como cliente, representado por la sonrisa de la imagen, pero la sonrisa también es una flecha. La flecha señala de la A a la Z, indicando que Amazon lo tiene todo de principio a fin.

Otro buen ejemplo es el logo de Tostitos. Éste es un logo muy social, como puede ver en la figura 6.7.

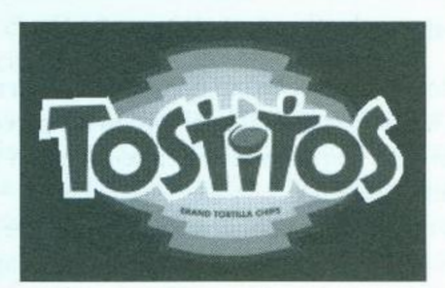


Figura 6.7. *¿Viendo este logo siente ganas de compartir una patata con alguien?*

Las dos letras T del centro del logo son dos personas compartiendo una patata sobre un bol de salsa. En 2004 la empresa envió una nota de prensa que decía: "Tostitos juega un papel como 'aperitivo social', ayudando a crear conexiones entre la familia y los amigos, ya sea en una fiesta, el día del 'gran partido' o en sencillas reuniones diarias. El nuevo logo retrata esta idea de la creación de conexiones".

Estos ejemplos son sólo una pequeña parte del uso del encuadre en el marketing. El encuadre no sólo consiste en imágenes; sobre todo tiene que ver con el valor que "el objetivo percibe".

La percepción que un objetivo tiene de un objeto puede aumentar o disminuir su valor. Ponga por caso una tienda de ropa exclusiva. Cuando entra todo está colgado ordenadamente, bien planchado y perfecto. La percepción puede ser justificar el precio exorbitante de la etiqueta. Sin embargo, si coge una de esas corbatas o camisas y la lleva a una tienda de saldos y la tira dentro de una gran caja llena de ropa marcada con un cartel que dice "descuento del 75 por 100", su percepción del valor de ese objeto disminuirá. Los gurús del marketing utilizan este fenómeno en un intento de encuadrar la percepción del valor del público. Muchas empresas han sido tan exitosas empleando el encuadre que la gente ha llegado a acuñar frases utilizando el nombre de sus productos.

Por ejemplo, todo el mundo dice: "Cuando te vayas de acampada no olvides el *camping gas*", incluso aunque el hornillo en cuestión no sea de esa marca concreta. Campingaz es el nombre de una empresa, no de un tipo de artilugio.

Un ejemplo más reciente es emplear el término "Google", independientemente del motor de búsqueda que se esté empleando ("¿Lo has buscado en Google?"), porque Google se ha convertido en un sinónimo de buscar en la Web. Y la gente dice: "Pásame un kleenex, por favor", cuando lo que quiere es un pañuelo.

Otros nombres que quizá no sepa que son marcas (a no ser que sea de la generación en la que se introdujeron) son:

- Aspirina es un producto de Bayer.
- Tirita es una marca registrada de Johnson & Johnson.
- Frisbee es una marca registrada de Wham-O.

Todos esos productos se han hecho tan populares que su referencia en la mente de las personas llega a abarcar a cualquier producto parecido. Yo nunca tomo Aspirina, suelo utilizar otra marca, pero siempre pido "un par de aspirinas", me dan otra marca y quedo satisfecho.

Existen volúmenes enteros que hablan sobre el encuadre, pero es necesario resumir algunos principios fundamentales para que pueda emplearlos como auditor de seguridad. Esta información le explica lo que es el encuadre y cómo se utiliza en distintas áreas de la vida. Antes de pasar al ruedo de la ingeniería social, eche un vistazo a los distintos modelos de alineamientos.

Los cuatro modelos de alineamiento

Dos investigadores, David Snow de la Universidad de Arizona y Robert Benford de la Universidad de Nebraska, escribieron un artículo llamado "Clarifying the Relationship Between Framing and Ideology in the Study of Social Movements"

(Clarificación de la relación entre el encuadre y la ideología en el estudio de los movimientos sociales): www.social-engineer.org/resources/book/SNOW_BED.pdf.

Snow y Bedford afirman que, cuando los encuadres individuales se asocian en congruencia y complementariedad, se produce el "alineamiento", produciendo una "resonancia del encuadre", que es fundamental en el proceso de un grupo transitando de un encuadre a otro. Snow y Bedford señalaron cuatro condiciones que afectan al encuadre:

- **"La robustez, totalidad y rigurosidad del encuadre":** Snow y Bedford identificaron tres tareas del encuadre y el grado en que estas tareas se atienden determina cuánto se involucra cada participante.

  Los tres pasos son:

  1. Diagnosticar el encuadre en busca de problemas.
  2. Analizarlo para alcanzar soluciones.
  3. Si se tiene éxito, realizar una llamada a la acción.

     Cuanto más esfuerzo se realice, mayores opciones tendrá la persona de atraer hacia su encuadre a los demás.

- **"La relación entre el encuadre propuesto y el sistema de creencias mayor":** La gente tiende a descartar encuadres o encuadres propuestos si no existe una relación con una creencia fundamental o un valor de su sistema de creencias.

  Intentar convencer a una persona que cree que comer carne es una crueldad con los animales, para que vaya a una hamburguesería a aprovechar una oferta, fracasará sin duda. El encuadre debe encajar en el sistema de creencias de la persona para tener éxito (a no ser que la meta sea utilizar el encuadre precisamente para cambiar sus creencias); es fundamental para tener éxito.

  Los polémicos anuncios antitabaco fueron un intento a gran escala de lograr un cambio de encuadre. Unos voluntarios apilaron bolsas de cadáveres frente a la puerta del edificio de una empresa tabacalera. Las bolsas representaban la gente que muere cada minuto, hora y día por culpa del tabaco. La pretensión era alterar el encuadre de los partidarios del tabaco haciéndoles pensar en el número de muertes que provoca el tabaco.

- **"Relevancia del encuadre para la realidad de los participantes":** El encuadre debe ser relevante para el objetivo. Debe ser comprobable y acreditable, al estar relacionado con las experiencias del objetivo.

No puede pretender utilizar un encuadre de marketing para animar a la gente a que haga un crucero de lujo en un lugar donde la gente no tiene dinero para comer cada día. No importa lo bueno que sea empleando el encuadre, fracasará. Para que el encuadre se alinee con el objetivo, no sólo debe ser relevante, debe ser demostrable para tener valor, aunque sólo sea en la mente del objetivo.

Por ejemplo, en 2007 una fuente de información muy popular y fiable, *Insight Magazine* (que es propiedad de la misma empresa dueña de *The Washington Times*), informó que el entonces candidato a la presidencia Obama había acudido a un colegio musulmán que era conocido por enseñar el islam desde un punto de vista radical y fundamentalista. Cuando apareció esta noticia muchos la creyeron de inmediato. ¿Por qué? Porque encajaba en el marco de su realidad, parecía creíble y provenía de una fuente "fiable".

CNN, otra fuente de noticias de confianza, envió a unos investigadores, descubrieron que la noticia era falsa e informaron de ello.

Éste es un buen ejemplo de alteración del marco mental de las personas sobre un tema utilizando una fuente muy fiable: los medios de comunicación. La gente que quería creer que Obama era un musulmán radical creyó la historia y la noticia corrió como la pólvora. Cuando la investigación demostró que la noticia era falsa, de nuevo se alteró el pensamiento de mucha gente.

- **"Ciclos de protesta; el punto en el que el encuadre emerge en el calendario de la era actual y de las preocupaciones con el cambio social":** Lo que sucede en el mundo puede afectar a un encuadre social. Si hace unos años se hubieran propuesto los escáneres corporales en los países occidentales, la idea se habría descartado.

  Los activistas por la privacidad habrían luchado contra esta idea y habrían ganado, simplemente utilizando la idea de que alguien pueda ver sus partes privadas y potencialmente pueda guardar las imágenes para burlarse o acosar a alguien. Estos argumentos habrían superado a los intentos de comercialización de los creadores de esas máquinas. Sin embargo, después de los ataques del 11 de septiembre y el subsiguiente aumento de la actividad terrorista, esas máquinas se están instalando en aeropuertos de todo el mundo, a pesar de las protestas de los activistas que incluso tienen de su lado el poderoso argumento de las leyes contra la pornografía infantil.

  ¿Por qué? El encuadre social de cómo mantenerse seguro ha sido alterado, permitiendo la entrada de un nuevo tipo de decisiones.

Snow y Benford afirman que, cuando se construyen los encuadres adecuados como se describe en estos cuatro puntos, se pueden lograr cambios a gran escala en la sociedad tales como los necesarios para los movimientos sociales, a través del alineamiento. Sus estudios se centran en la sociedad en conjunto, pero estos mismos principios también son efectivos a menor escala, incluso a nivel individual.

Esta explicación sólo abarca el proceso del alineamiento; de hecho, pueden darse cuatro tipos de alineamiento diferentes una vez que estas cuatro condiciones se cumplen. Aunque muchos de estos aspectos se orientan hacia grupos de encuadre en su totalidad, las siguientes secciones explican estos cuatro alineamientos a nivel personal mostrando cómo utilizarlos en su labor como ingeniero social o simplemente como una persona que quiere alinear sus encuadres con los demás. Imagine que desea alinear su meta de entrar en un edificio con el encuadre del guardia de seguridad que está diseñado para prohibirle el paso. Alinear el encuadre del guardia con su pretexto puede asegurarle el éxito en la acción.

Una cosa que conviene recordar sobre los encuadres es que nunca se crean de la nada. Los encuadres siempre parten de códigos culturales existentes que implican el núcleo de las creencias y experiencias de una persona.

El puenteo del encuadre

El *Cathie Marsh Centre for Census and Survey* (Centro Cathie Marsh de censos y sondeos) define el puenteo como el enlace de dos o más encuadres ideológicamente congruentes pero desconectados a nivel estructural, respecto a un tema concreto. El puenteo no consiste en hacer creer a la gente que su encuadre es mejor que el suyo, sino en comprender su encuadre tan profundamente que pueda encontrar el punto de conexión. Entonces, puede utilizar esa conexión para atraer al objetivo hacia su encuadre.

Puede darse una situación en la que quiera acceder a un edificio, una zona o una información importante. Su encuadre es que quiere que esto suceda. El encuadre de la persona a la que aborda no tiene por qué ser detenerle; puede que ni siquiera sepa lo que está intentando hacer. Si aborda la situación con esa actitud, puede alertarlo, acabando de esta forma con sus posibilidades.

Al comprender el trabajo y la conducta del objetivo puede comprender su encuadre mental y encontrar un enlace que haga más fácil la transición a su encuadre.

¿Cuál es su pretexto? ¿Cómo trataría la persona a la que va a abordar a alguien como su pretexto? Debe entender esto para tener éxito. El guardia tratará de distinta manera a un comercial que al reponedor de la máquina de refrescos. Comprender el encuadre del objetivo implica saber cómo tratará a su pretexto.

Otro ejemplo consiste en pensar cómo quiere que le vean los demás. Puede que como alguien tranquilo, equilibrado, inteligente o confiado. Un atleta quiere mostrarse calmado y fuerte. Un cómico quiere resultar gracioso. Todo esto son encuadres con los que alguien quiere que los demás se alineen.

En el caso del cómico, ¿qué sucede si hay alguien en la audiencia que no le considera gracioso, inteligente o seguro de sí mismo? Puede que su encuadre afecte a la audiencia y ésta se muestre descontenta o desinteresada. Si el cómico persiste en su propio encuadre puede que atraiga a algunas personas a su alrededor pero, hasta que no profundice e intente comprender el origen de la situación, no será capaz de alinear los dos encuadres y atraer a la persona descontenta hacia el suyo. El cómico que consigue manejar una situación de este tipo aleja sus miedos y acaba sacando partido.

La técnica de alineamiento por puenteo puede ser una de las más poderosas que pueden emplearse en una auditoría de seguridad, pero requiere cierta preparación para realizarla correctamente.

Este tipo de alineamiento puede emplearse para ayudar al objetivo a tender un puente entre lo que ve y lo que debe creer a través de un pretexto determinado. Una vez más, recuerde el ejemplo del técnico de asistencia que quiere acceder a un edificio. La vestimenta, las herramientas y el lenguaje deben coincidir con el encuadre que el objetivo espera de un técnico. Si lo consigue, se crea el puente y el alineamiento tiene lugar.

La amplificación del encuadre

Según Snow, la amplificación del encuadre se refiere a "la aclaración y la estimulación de un encuadre interpretativo que recae en un asunto, problema o evento particular". En otras palabras, se amplifican los valores o creencias del objetivo. Al centrarse en esos valores puede encontrar un área en la que pueden alinearse ambos encuadres o, al menos, hacer creer al objetivo que existe ese alineamiento.

Ésta es la forma de alineamiento más básica de las cuatro porque se trata, sobre todo, de un método de mantenimiento. Consiste en acentuar, incrementar o puntualizar que un evento es más importante que otros, lo que permitirá conectar fácilmente este evento con otros.

Podemos ver un ejemplo de amplificación del encuadre si profundizamos un poco en el ejemplo anterior de los escáneres corporales. Esos escáneres se han vendido como un elemento disuasorio para los terroristas. El encuadre bajo el que se han vendido es que la reciente actividad terrorista requiere un producto de este tipo, que ha aparecido para cubrir esa necesidad. Al investigar estos productos, descubrimos que fueron fabricados, comercializados y rechazados mucho antes de los ataques del 11 de septiembre.

Al utilizar los ataques del 11 de septiembre combinados con el miedo a volar que desarrolló mucha gente, esas empresas consiguieron relacionar su encuadre con el miedo que mucha gente sentía y de esta manera consiguieron apoyo para implementar estos aparatos en aeropuertos por todo el mundo.

Otro de los efectos de la amplificación es que puede emplearse para desdibujar el encuadre y provocar que la gente se distancie de sus propias creencias. Por ejemplo, mucha de la gente que creía en la privacidad y en el derecho a elegir cómo ser escaneada ha sido desviada a un encuadre diferente por los fabricantes de los escáneres corporales, afirmando que ciertos aspectos de los otros métodos de escaneo eran inseguros o incompletos, y para demostrarlo presentaron historias como la del individuo que llevaba una bomba en la ropa interior. Este tipo de tácticas amplifica la creencia de que el nuevo encuadre es más seguro utilizando la falta de seguridad de los otros métodos.

Un ingeniero social puede utilizar este alineamiento de muchas maneras. Por ejemplo, puede necesitar convencer a un guardia para que le deje acceder a la zona de los contenedores. El pretexto de trabajar para la empresa de recogida de basuras funciona bien por sí mismo, pero funcionará aún mejor si argumenta que uno de los contenedores está estropeado, lo que conlleva una responsabilidad por parte de la empresa. Amplificar ese encuadre puede conseguir que el guardia de seguridad se alinee con la idea de que la mejor solución es permitirle el acceso.

La extensión del encuadre

"Las extensiones del encuadre son movimientos para incorporar participantes extendiendo los límites del encuadre propuesto para abarcar los puntos de vista, intereses y, sobre todo, los sentimientos de un grupo". En otras palabras, al entender los límites de su encuadre para abarcar los intereses de su objetivo, logrará alinearlos.

Por ejemplo, existe la posibilidad de que los grupos que apoyan causas ecológicas o "verdes" puedan extender su encuadre hacia los movimientos antinucleares, afirmando que están preocupados por los riesgos para el medio ambiente.

Sin embargo, cuando se utilizan las extensiones de encuadre se corre el riesgo de debilitar la postura respecto al encuadre original y se puede perder cierto nivel de atracción. Esto puede suceder al incluir demasiadas extensiones en un mismo encuadre provocando su debilitación y la pérdida de interés.

Incluso a nivel personal, lo más simple es lo mejor. Cuando emplee esta táctica hágalo con sencillez y de modo que sea fácil de seguir. No cree una red de conexiones tan enrevesada que el objetivo pierda el interés.

Esta técnica se puede utilizar a través de las maniobras de obtención de información explicadas en el capítulo 3. Para reunir información sobre un objetivo, en lugar de mostrarse interesado en eso, puede emplear una charla informal en una fiesta o utilizar el pretexto de un periodista. De este modo, obtendrá el "derecho" a solicitar cierta información que de otra forma habría sido muy difícil de conseguir.

Transformación del encuadre

"La transformación del encuadre es un proceso necesario cuando los encuadres propuestos no concuerdan con, o resultan contrarios a los estilo de vida convencionales y a los encuadres interpretativos existentes".

En otras palabras, el ingeniero social ofrece nuevos argumentos que apuntan a las razones de que su encuadre sea mejor en un intento por transformar y trasladar los pensamientos o creencias de un objetivo desde donde están a donde el ingeniero social quiere llevarlos.

Cuando sucede esta transformación del encuadre, son necesarios nuevos valores y conocimientos para mantener a la gente involucrada y mantener su apoyo. Este tipo de transformación se llevó a cabo a gran escala en los años setenta, cuando el movimiento conservador se transformó en un movimiento más progresista y ecologista.

En menor escala, las transformaciones de encuadre suceden a diario a través de las conversiones religiosas, en las que el encuadre o sistema de creencias de la persona es alterado, cambiado y transformado para alinearlo con el nuevo encuadre de pensamiento que ofrece la nueva religión.

No es fácil transformar el encuadre de una persona; es una de las tácticas de alineamiento más complicadas de poner en práctica porque requiere:

- **Tiempo:** Cambiar el sistema de creencias de una persona no es un proceso rápido y puede requerir la utilización de otras técnicas de alineamiento y mucho tiempo para que funcione.
- **Esfuerzo:** Saber de dónde viene el objetivo y a dónde quiere llevarle son sólo los primeros pasos. ¿Cuáles van a ser sus objeciones y sus bloqueos mentales? Descubrirlo puede llevarle un gran esfuerzo.
- **Formación:** El conocimiento es poder. Debe ayudar al objetivo a entender el nuevo encuadre al que quiere "convertirlo".
- **Lógica:** La formación debe ser lógica y no estar compuesta únicamente por sentimientos. El objetivo debe ser capaz de razonar y racionalizar la acción que está a punto de llevar a cabo. El único modo de conseguirlo es a través de la lógica.

- **Lazos emocionales profundos:** El conocimiento es lo que prepara a la persona para la acción, la lógica le convence de que es bueno realizar esa acción pero la emoción es lo que hace que la acción tenga lugar. Si se muestra emotivo en relación a su "causa" el objetivo sentirá esa emoción. Asegúrese de que los sentimientos que está expresando encajan con el pretexto. Si su pretexto es un orientador y aparece vestido como una animadora evitará que el objetivo pueda alinearse.

Si es capaz de alinear a otros a su encuadre y de alinearse usted con los de ellos, incentivará a la gente para que haga lo que les pide. Aunque los cuatro métodos de alineamiento son poderosos, el ingeniero social que tiene éxito con la transformación del encuadre posee un poder ilimitado.

Continúe leyendo para poder descubrir cómo se aplican estas técnicas en ingeniería social.

Utilizar el encuadre en ingeniería social

A lo largo de este capítulo, he mencionado varias formas de emplear las técnicas del encuadre. Algunos de estos métodos son tan poderosos que al perfeccionarlos se convertirá en un maestro de la persuasión.

Hay cuatro cosas que debe saber sobre el encuadre para poder emplearlo en ingeniería social. Esto le ayudará a comprender claramente cómo funciona el encuadre y cómo utilizarlo.

Recuerde lo que es el encuadre. Es una estructura conceptual que nuestras mentes utilizan en el pensamiento. Esta información es importante, porque su meta será o bien crear un nuevo encuadre o alienarse con el encuadre de otra persona o atraer al objetivo hacia el suyo.

Cualquiera de estas metas necesita observar las cuatro reglas que se describen a continuación.

Regla 1: Todo lo que diga evocará un encuadre

La mente humana funciona formándose imágenes. No puede cambiar este hecho, pero puede utilizarlo en su propio beneficio.

Si empiezo a hablarle de su jefe, su mente se lo imaginará. Si le describo una situación en la que su jefe estaba en la calle hablando muy enfadado por el teléfono móvil, imaginará su cara de enfado, su lenguaje corporal y sus palabras. No será capaz de controlarlo y ese encuadre mental provocará ciertas emociones y reacciones.

Formar una imagen con palabras es un modo muy efectivo de emplear el encuadre. Eligiendo cuidadosamente las palabras, provocará que el objetivo imagine ciertas cosas y empiece a moverse hacia el encuadre que desea.

¿Alguna vez ha conocido a alguien a quien considera un gran narrador? ¿Por qué? ¿Qué hacía que fuera tan bueno? Era capaz de ilustrar lo que decía, hacer que imaginara las cosas, manteniéndole intrigado y atento. Esta habilidad es muy importante para un ingeniero social. No significa que siempre tenga que hablar como si estuviera contando una historia genial, pero debe prestar atención a las palabras que elige porque tienen el poder de crear imágenes en la mente de su objetivo.

Aquí tiene un ejemplo sencillo: puedo decirle que ayer cené espaguetis. Si la última vez que probó ese plato la experiencia no fue buena será difícil la conexión mental.

¿Qué pasaría si le digo que ayer mi mujer preparó unos tomates con especias cultivados en nuestro jardín? Tenían ajo, albahaca y orégano y un ligero toque de vino tinto. Los sirvió sobre un plato espaguetis con un poco de pan de ajo.

Aunque no le guste mucho la pasta, ahora se está imaginando un plato de restaurante de calidad. Ésta es la manera en que tiene que seleccionar las palabras con sus objetivos. Debe ser descriptivo, evocador e ilustrativo. Aunque es necesario no resultar demasiado teatral. La meta es crear una imagen precisa, no atraer demasiado la atención hacia usted.

Regla 2: Las palabras que se definen dentro de un encuadre evocan el encuadre mental

No es necesario que utilice las palabras exactas para conseguir que el objetivo imagine lo que desea. Por ejemplo, ¿qué piensa cuando lee la siguiente frase?

"Vi al insecto luchando para escapar de la red, pero no pudo. Momentos después, estaba envuelto formando un capullo, preparado para la cena".

Observe que no he tenido que mencionar una araña para hacerle pensar en ella. Si quiero que piense en una araña no es necesario que diga la palabra "araña". Esta poderosa regla le da la posibilidad de controlar los pensamientos del objetivo empleando el estilo indirecto.

Toastmasters, la organización internacional especializada en las habilidades del habla de las personas, enseña a sus miembros a conmover a su audiencia haciendo que se impliquen sus emociones. Al contar una historia que consiga que el objetivo se forme una imagen a la vez que se involucra emocionalmente, solidificará su posición de control en esa conversación.

Una vez más, emplear este método requiere planificación. Un aspecto importante de esta regla es que, mientras el cerebro del objetivo está procesando esta información, usted la está alimentando. Al generar las imágenes mentales puede

introducir pensamientos e ideas. Al contrario que en el ejemplo del plato de pasta, en este caso otorga al objetivo la libertad de imaginar otra cosa. Podía haber terminado la historia del plato de pasta diciendo: "Mi mujer lo sirvió sobre un plato de pasta. ¿Qué tipo de pasta? No te lo digo, tendrás que imaginarlo" y, cuando su cerebro empiece a hacerlo, puedo decir: "Cuando la enrollaba con el tenedor la salsa era tan compacta que no se despegaba".

Esta descripción forma la imagen mental de los espaguetis. ¿Qué otro tipo de pasta se enrolla? (ya sé que hay otras, pero con esto puede ver lo que quiero decir).

Regla 3: Negar el encuadre

Si le digo que no se imagine una araña en una red, primero su cerebro tendrá que imaginar la araña para después dar la orden de no hacerlo.

Está técnica de negación es poderosa. Decirle a un objetivo que tenga cuidado, que esté atento a algo, le coloca de inmediato en el encuadre que quiere. Esta técnica se emplea a menudo en ingeniería social. En una entrevista que hice a un grupo de profesionales, todos coincidían en que esta técnica funciona muy bien.

Durante una auditoría dejé unas cuantas llaves USB perdidas por el edificio que contenían código malicioso que quería que alguien de la empresa ejecutara. Me acerqué a un empleado que confiaba en mí y dije: "John, parece que han publicado una nota para que estemos atentos a unas llaves USB que se han perdido. Ahora las están buscando". Da la casualidad de que estaba allí interpretando el papel del conserje y había dejado caer las llaves USB con código malicioso. Al decirle a la gente que las buscara, estaba plantando la semilla de mi acción. Este tipo de frase niega la preocupación que podía sentir al encontrar una llave USB y consigue que la conecte a su ordenador para comprobar de quién es.

Regla 4: Conseguir que el objetivo piense en el encuadre refuerza ese encuadre

Cada vez que el cerebro se centra o piensa en algo, se refuerza esa idea. Cuanto más consiga que el objetivo imagine el encuadre al que quiere conducirlo, más sencillo será reforzarlo y llevarlo hasta él.

Repase el capítulo 2 sobre los modelos de comunicación y analice el asombroso efecto que tienen los mensajes que desarrolla un ingeniero social.

En cierta ocasión, realicé un viaje a la India. No recuerdo exactamente lo que sucedió, pero el presidente George W. Bush había perdido el favor del público europeo. Estaba viendo las noticias y aparecieron imágenes de algunas personas en las calles de un país europeo que sostenían unos muñecos que representaban a Bush. Envolvieron los muñecos en banderas de Estados Unidos y les prendieron fuego.

Era una escena impactante y hablando por teléfono con mi mujer esa tarde le dije: "Qué locura lo que está sucediendo en Europa, ¿verdad?".

No sabía nada del asunto. ¿Por qué? Los medios de comunicación son maestros de la manipulación.

Se puede aprender mucho observando cómo emplean estas técnicas. Empleando la omisión o dejando fuera algunos detalles de la historia o la historia completa, pueden conducir a la gente a una conclusión que considere propia, pero que en realidad es la conclusión del medio de comunicación.

Los ingenieros sociales pueden hacer esto. Omitiendo detalles y filtrando sólo los que le interesan, puede crear el encuadre al que quiere conducir al objetivo.

Otra táctica empleada por los medios de comunicación es el "etiquetado". Cuando quieren marcar algo como positivo dicen cosas como "la gran defensa de..." o "nuestra saneada economía". Estas frases crean imágenes mentales de estabilidad y salud y ayudan a llegar a conclusiones positivas. Lo mismo se aplica para realizar encuadres negativos. Etiquetas como "terrorista islámico" o "teorías conspirativas" forman una imagen muy negativa.

Puede emplear estas habilidades para etiquetar las cosas con palabras descriptivas que llevan al objetivo al encuadre que desea. En cierta ocasión en que quería entrar en un edificio, pasé por la caseta del guardia de seguridad como si perteneciera a aquel lugar. Me detuvieron al instante. Miré asombrado al guardia y con un tono de disculpa dije: "Oh, ayer este guardia tan amable, Tom, comprobó mis datos y me dejó pasar. Por eso he dado por hecho que seguía en la lista".

Al etiquetar al guardia anterior como "amable" puse inmediatamente al guardia en el encuadre que quería. Si quería recibir una etiqueta igual de favorecedora, tendría que ser amable conmigo también.

El etiquetado es efectivo porque distorsiona la realidad pero no tanto como para falsearla, por lo que se mantiene creíble. Un auditor de seguridad puede formar la impresión deseada dando la sensación de que está siendo objetivo.

Leí un informe llamado "Status Quo Framing Increases Support for Torture" (El encuadre existente aumenta el apoyo a la tortura), escrito por Christian Crandall, Scott Eidelman, Linda Skitka y Scott Morgan, todos ellos investigadores de distintas universidades.

Revelaron una información muy interesante que me intrigó. En Estados Unidos parece que mucha gente está en contra del uso de la tortura en tiempo de guerra como una táctica para obtener información. El propósito de este estudio era intentar que un grupo de personas considerara que la tortura es aceptable, presentando el mensaje de otra forma.

Tomaron un grupo de muestra de 486 personas y les pidieron que leyeran dos párrafos.

El primero decía:

La utilización del estrés para interrogar a sospechosos por parte de las fuerzas de Estados Unidos en el Medio Oriente está en las noticias. Este tipo de interrogatorio es nuevo; según algunos informes, es la primera vez que se utiliza a gran escala en las fuerzas armadas. Se han empleado muchos métodos diferentes, como atar al detenido a una tabla y hundirlo en agua, meter al detenido al revés en un saco de dormir y colgar a los detenidos durante largos periodos de tiempo en posiciones dolorosas. También se ha mantenido despiertos y solos a los detenidos durante varios días.

Este párrafo crea la imagen de que éstas son técnicas "nuevas" empleadas por el gobierno para obtener información. El segundo párrafo dice:

La utilización del estrés para interrogar a sospechosos por parte de las fuerzas de Estados Unidos en el Medio Oriente está en las noticias. Este tipo de interrogatorio no es nuevo; según algunos informes, se utiliza en las fuerzas armadas desde hace más de 40 años. Se han empleado muchos métodos diferentes, como atar al detenido a una tabla y hundirlo en agua, meter al detenido al revés en un saco de dormir y colgar a los detenidos durante largos periodos de tiempo en posiciones dolorosas. También se ha mantenido despiertos y solos a los detenidos durante varios días.

La situación en esta versión es idéntica, excepto la segunda frase que se sustituye por "Este tipo de interrogatorio no es nuevo; según algunos informes, se utiliza en las fuerzas armadas desde hace más de 40 años".

¿Cuáles fueron los resultados de este cambio de encuadre, entre unos métodos nuevos y otros que se emplean desde hace décadas?

El papel describe las mediciones de los investigadores. Siete elementos formaron el conjunto básico de variables dependientes. Estos elementos se correspondían con una escala de "botones" de siete puntos, en la que los botones se etiquetaban como muy en desacuerdo, moderadamente en desacuerdo, ligeramente en desacuerdo, incierto, ligeramente de acuerdo, moderadamente de acuerdo y muy de acuerdo. La puntuación más alta indicaba mayor acuerdo con los elementos puntuados.

¿La conclusión?: "La manipulación de la situación tuvo un efecto en la evaluación global de la tortura: cuando fue descrita como una práctica antigua, se evaluó de manera "más positiva"; al hacer ver que la tortura formaba parte del statu quo de las interrogaciones aumentó el apoyo individual y la justificación para el empleo de esta táctica".

Simplemente cambiando una pequeña parte del encuadre los investigadores consiguieron alinear a un grupo considerable de personas para hacerles estar de acuerdo (en su mayoría) en que la tortura era una política aceptable.

El informe continuaba señalando: "Se pueden aplicar a muchos terrenos y pueden afectar al juicio, a la toma de decisiones, a la estética y a las preferencias políticas". Concluyendo que: "Cambios relativamente modestos en la forma en que se presentan las opciones éticas y los dilemas de valores pueden tener un profundo efecto en la elección política".

Este experimento demuestra el gran poder del encuadre, que puede cambiar las creencias, los juicios y las decisiones que puede tomar la gente durante muchos años. Como ingeniero social, ésta no suele ser la meta. No está tratando de transformar a la gente; sólo pretende que realice cierta acción que pensando un poco habría decidido no realizar. Aplicar las cuatro reglas del encuadre y planificar mucho hará del encuadre una fuerza poderosa a tener en cuenta. Éste es motivo por el que, desgraciadamente, los ingenieros sociales maliciosos utilicen esta técnica a diario. En los países occidentales sobre todo, la gente está adiestrada para aceptar que le digan qué y cómo pensar.

Si hace 15 años le hubiera dicho que prácticamente todos los programas de televisión consistirían en gente real haciendo cosas reales, se habría reído de mí. ¿Por qué? Porque pensar en ese tipo de programas le habría parecido aburrido y estúpido. No obstante, en 2006 el periódico *Los Angeles Times* afirmó que el número de *reality shows* se había incrementado en un 128 por 100 (`http://articles.latimes.com/2010/mar/31/Business/la-fi-ct-onlocation31-2010mar31`) y no ha descendido mucho desde entonces y, debido a que verlos es lo que está de moda y nos dicen que son buenos y divertidos, todo el mundo lo hace. Estos programas son un buen ejemplo de cómo se puede conseguir que a la gente le parezca buena una cosa que sólo unos años antes habría considerado estúpida.

El encuadre es una forma de arte y cuando se combina con la ciencia de la comunicación y la influencia puede convertirse en una fuerza poderosa en las manos de un ingeniero social habilidoso, que puede presentar la información de forma que resulte "fácil" que el objetivo se alinee con él, realice una acción sin sentirse culpable o altere su percepción de la realidad. El encuadre y la influencia son elementos clave de la ingeniería social, pero existe otro concepto que normalmente se asocia con los "rincones más oscuros" de este campo. En la introducción de este libro, mencionamos que profundizaríamos en esos rincones; la siguiente sección presenta la información que cambiará la forma en que concibe la influencia.

La manipulación: controlar al objetivo

La manipulación es considerada por mucha gente como un tema siniestro al que se teme por el modo en que normalmente se retrata. Para explicarlo pueden servir algunas definiciones encontradas en Internet:

- "Ejercer una influencia astuta o taimada, normalmente para beneficio propio".
- "Influenciar o controlar con artimañas o astucia".
- "Controlar (a otros o a uno mismo) o influenciar con habilidad, normalmente para beneficio propio".

Puede ver claramente por qué a tantos ingenieros sociales se les cae la baba con este tema. ¿Puede imaginar ser capaz de utilizar sus habilidades para controlar o influenciar a alguien para su propio beneficio?

Desde algo tan siniestro como el lavado de cerebro hasta las sutiles insinuaciones de los vendedores, las tácticas de manipulación son algo que todo auditor de seguridad debe estudiar y perfeccionar. El propósito de la manipulación es superar al pensamiento crítico y al libre albedrío de sus objetivos. Cuando el objetivo pierde la habilidad para tomar una decisión en base a procesos informados, la persona que le manipula puede alimentarlo con sus ideas, valores, actitudes o razonamientos.

La manipulación se utiliza de seis maneras que se cumplen tanto en el lavado de cerebro como en cualquier manipulación menos dañina. Vamos a repasarlas rápidamente antes de profundizar en esta sección.

- **Conseguir que el objetivo sea más sugestionable:** En su versión más radical, la privación de sueño o comida consigue que el objetivo sea más sugestionable. En un plano menos extremo, las insinuaciones sutiles que crecen en intensidad hacen que el objetivo sea más fácil de sugestionar.
- **Hacerse con el control del entorno del objetivo:** Esta técnica puede implicar muchas cosas, desde controlar el tipo y la cantidad de información a la que el objetivo tiene acceso hasta elementos mucho más sutiles como acceder a los sitios Web de medios sociales del objetivo. Acceder a los medios sociales le permite observar las formas de comunicación del objetivo, a la vez que ejerce control sobre la información que recibe.
- **Crear la duda:** Desestabilizar y minar el sistema de creencias del objetivo puede ser muy efectivo para manipularlo en cierta dirección. Debe hacerse con discreción. No puede simplemente irrumpir y comenzar a degradar a su objetivo; en lugar de eso, puede afectar a su habilidad para tomar decisiones racionales cuestionando las normas que sigue, su trabajo o sus creencias.
- **Crear un sentido de impotencia:** Esta técnica verdaderamente maliciosa se utiliza en los interrogatorios en tiempo de guerra para lograr que el objetivo pierda la confianza en sus convicciones. Como ingeniero social puede utilizar esta táctica presentando los "hechos" que ha recibido de alguien con autoridad y creando con ello un sentimiento de impotencia.

- **Provocar respuestas emocionales intensas en el objetivo:** Estas respuestas pueden incluir dudas, culpabilidad, humillación, etc. Si las emociones son lo suficientemente intensas, pueden cambiar su sistema de creencias completo. En el contexto de una auditoría de seguridad es necesario tener cuidado para no provocar emociones negativas dañinas, pero utilizar tácticas que provoquen una respuesta emocional basada en el miedo a perder o en el castigo puede ser beneficioso para lograr su meta.
- **Intimidación:** El miedo al dolor físico o a otras circunstancias nefastas puede utilizarse para que el objetivo ceda a la presión. De nuevo, la mayoría de ingenieros sociales no seguirá este camino, a no ser que esté empleando como táctica el espionaje empresarial, pero en una auditoría normal, esta táctica utiliza la percepción de autoridad para generar sentimientos de miedo y de pérdida potencial.

No obstante, la mayoría de las ocasiones la manipulación no es tan radical. En un nivel muy básico, imagine que está en una habitación llena de gente y alguien grita su nombre. ¿Cuál es su reacción? Normalmente girará y contestará: "¿Sí?". Ha sido manipulado, aunque no necesariamente de forma negativa.

A nivel psicológico la manipulación es aún más profunda. Observe el proceso que ha tenido lugar para que se diera la reacción que acabamos de describir. Su cerebro escucha su nombre y automáticamente formula una respuesta ("¿sí?"). La conexión entre la respuesta del cerebro y la respuesta vocal es muy corta. Incluso si no formula una respuesta vocal o si la llamada se refería a otra persona, cuando se hace una pregunta su cerebro responde.

Simplemente estar cerca de dos personas conversando y escuchar una pregunta hará que su mente formule una respuesta. Puede ser una imagen o un sonido. Si escucha a dos personas hablando sobre el aspecto físico de otra, creará una imagen mental. Si escucha a alguien contar un chiste de un pollo cruzando una carretera, imaginará el pollo, la carretera y la escena completa.

Este tipo de manipulación es sólo el principio de sus posibilidades. Otra táctica de manipulación es el "condicionamiento". La gente puede ser condicionada para relacionar determinados sonidos o acciones con sensaciones y emociones. Si cada vez que se menciona algo positivo la persona escucha el clic de un bolígrafo, en poco tiempo se puede condicionar al objetivo para que asocie ese sonido con un sentimiento positivo. El ejemplo más clásico de condicionamiento es el experimento de Ivan Pavlov conocido como el perro de Pavlov, explicado en el capítulo 5. La pregunta que surge es si se puede utilizar este tipo de táctica con la gente. Aunque hacer salivar a la gente no es una prioridad de la ingeniería social (pero podría ser gracioso), ¿existen maneras para condicionar al objetivo para que reaccione a grupos de estímulos del modo en que quiere que lo haga?

Para encontrar una respuesta, lea las siguientes secciones, que proporcionan algunos ejemplos de manipulación en el marketing y los negocios para crear una base de discusión y análisis sobre el uso de la manipulación a nivel personal.

Retirar o no retirar

En mayo de 2010 el periódico *The Washington Post* publicó una historia interesante (`www.washingtonpost.com/wp-dyn/content/article/2010/05/27/AR2010052705484.html`). El fabricante de los medicamentos para niños Tylenol, Motrin, Benadryl y Zyrtec, entre otros fármacos de venta sin receta, descubrió una remesa defectuosa de Motrin pero no quiso llevar a cabo una retirada del producto debido al alto coste de dicha acción. ¿Qué fue lo que hizo la empresa?

Utilizó la manipulación. Recurrieron a los servicios de un grupo de contratistas para que fueran de farmacia en farmacia y compraran todo el Motrin que tuvieran, para destruirlo después. Por desgracia para ellos, el plan se estropeó cuando a uno de los contratistas se le cayó un documento en una de las farmacias en el que se explicaba el complot, que fue entonces denunciado a la Federal Drug Administration (la agencia de alimentos y medicamentos de Estados Unidos; FDA).

Por su parte, la FDA obligó a la empresa a retirar 136 millones de frascos solamente en una de las cuatro retiradas del producto que se ejecutaron. Desgraciadamente, ya era demasiado tarde porque se habían detectado 775 casos de niños afectados con reacciones adversas a este lote defectuoso, 37 de los cuales acabaron con la muerte del niño. En el informe no se pudo aclarar si las muertes fueron causadas por el Motrin defectuoso o por una reacción al medicamento, pero eso ahora es irrelevante.

Éste es un ejemplo muy siniestro de manipulación o, al menos, de un intento de manipulación. Con tal de salvar la imagen de la empresa estuvieron dispuestos a ignorar los procedimientos pertinentes y la seguridad de millones de niños de todo el mundo. Intentaron manipular al sistema y en el proceso hubo gente que perdió la vida. El documento que se le cayó al contratista explicaba sus órdenes de comprar el producto y no mencionar la palabra "retirada" en ningún momento.

Cuando la empresa fue descubierta se pusieron de manifiesto varias tácticas de manipulación interesantes. Desviaron la atención asegurando que la razón para actuar de aquel modo fue que sus expertos creían que no existía un peligro evidente para la salud de los niños.

Después de hacer esta afirmación, presentaron una disculpa formal y despidieron a seis altos ejecutivos. Entonces fue cuando empezó la verdadera manipulación. Cuando se le preguntó, la empresa negó que hubieran intentado hacer una "retirada fantasma", como fue denominada. La empresa quería realizar pruebas sobre la remesa

supuestamente defectuosa y los contratistas estaban comprando esa remesa para poder llevar a cabo las pruebas. Si hubieran encontrado problemas en el producto, habrían tomado las medidas oportunas. Esta empresa intentó utilizar una técnica de manipulación llamada "desviación", para desviar la atención de lo que estaban haciendo realmente, para que pareciera una acción más positiva de lo que era. Además, empleó una técnica de encubrimiento para manipular la opinión de aquéllos que cuestionaron su procedimiento, afirmando que la empresa estaba intentando analizar el producto para determinar si era necesario realizar una retirada del mismo.

Merece la pena explicar este tipo de manipulación porque la táctica de desviación se puede emplear a menor escala. Si le descubren en un lugar en que no debería estar, tener una coartada creíble puede servir para manipular al objetivo para que le deje vía libre. Desviar la atención del objetivo hacia cualquier cosa distinta del problema puede darle el tiempo suficiente para redirigir sus pensamientos. Por ejemplo, si es descubierto por un guardia de seguridad, en lugar de ponerse nervioso, puede mirarle tranquilamente y decir: "¿Sabe lo que estoy haciendo? ¿Se ha enterado de que se han perdido varias llaves USB con información importante? Tenemos que encontrarlas antes de que vuelva todo el mundo mañana. ¿Puede ir a comprobar los servicios?".

Es posible que hasta ahora no hubiera escuchado la historia del Motrin, lo que demuestra que la empresa hizo un buen trabajo manipulando (hasta ahora) a los medios de comunicación y al sistema de justicia para mantenerse alejada del foco de atención. En cualquier caso, esta historia muestra cómo pueden utilizarse la desviación y el encubrimiento para manipular a la gente.

La ansiedad curada por fin

En 1998, SmithKline Beecham, una de las empresas farmacéuticas más grandes del mundo, lanzó una campaña publicitaria diseñada para "educar" a la gente sobre algo que denominó "trastorno de ansiedad social". Presentaron 50 historias en prensa y sondeos con preguntas como: "¿Tiene usted un trastorno de ansiedad social?". Estas encuestas y sondeos iban dirigidos a "educar" a la gente sobre este trastorno y sobre cómo saber si lo padecía.

Unos meses más tarde, cambiaron el texto de la campaña de marketing, de "Paxil significa paz... con la depresión, el trastorno de pánico y el trastorno obsesivo convulsivo" pasaron a: "Les demuestra que pueden... el primer y único tratamiento aprobado para el trastorno de ansiedad social". Hacer este cambio le costó a la empresa alrededor de un millón de dólares.

En 1999, SmithKline Beecham lanzó una campaña en prensa y televisión anunciando que había encontrado la cura para el trastorno de ansiedad social, que denominaron Paxil. Utilizando la información que habían recabado con las

encuestas, la empresa compró espacios en algunos de los programas de televisión más exitosos del momento donde anunciaron datos estadísticos que afirmaban que diez millones de estadounidenses sufrían trastorno de ansiedad social, pero que ahora había esperanza para ellos.

En 2000, las ventas de Paxil supusieron la mitad del crecimiento del mercado entero: la empresa "se convirtió en la número uno del mercado de los inhibidores selectivos de recaptación de serotonina, entre los nuevos fármacos de venta con receta del año 2000". En 2001, consiguió la aprobación de la FDA para comercializar Paxil tanto para el trastorno de ansiedad generalizado como para el síndrome de estrés postraumático.

Los ataques del 11 de septiembre supusieron un incremento espectacular en las recetas de todo tipo de antidepresivos y fármacos contra la ansiedad. En aquel momento, los anuncios de Paxil lo señalaban como la respuesta a los incómodos sentimientos de miedo e indefensión que mucha gente sentía después de los ataques.

No estoy diciendo que el fármaco no funcione o que las intenciones de la empresa fueran malas, pero creo que éste es un caso especialmente interesante en el que la manipulación del mercado empezó con educación y acabó con un crecimiento enorme de ventas, creando nuevos trastornos por el camino.

Este tipo de montaje se emplea habitualmente en el mundo del marketing, pero se utiliza también en la política e incluso a nivel de relaciones personales, presentando un problema terrible, para luego presentar unos "hechos" que se consideran la prueba de que lo que se dice es cierto. En un episodio de *The Real Hustle*, Paul Wilson preparó un escenario en el que utilizaban a un personaje famoso para robar unos CD en una tienda. El dependiente detenía al famoso y esperaba a que llegara la policía. Entonces, entraba Paul, se identificaba como policía enseñando su cartera en la que no había nada más que una foto de sus hijos, "arrestaba" al famoso, llevándose los CD y el dinero de la caja como pruebas del caso y se iba sin despertar la más mínima sospecha. Esta historia es un buen ejemplo de manipulación mediante un montaje. Paul creó un problema (el ladrón famoso) y se presentó a sí mismo como la solución (el policía) al problema. Llevando esta táctica a cualquier otra situación, si consigue hacer ver lo buena persona que es, antes de formular su petición, ésta será mucho más fácil de aceptar para la persona que pretende manipular.

¡No puede obligarme a comprar eso!

Centros comerciales Kmart. Me veo tentado a dejar esta sección así, pero creo que voy a desarrollar el argumento un poco más. Kmart desarrolló una idea que denominó el "planograma", que es un diagrama que muestra a los minoristas

cómo colocar los productos en sus tiendas en base a los colores, los tamaños y otros criterios para poder manipular a sus clientes para que quieran comprar y gastar más.

Los planogramas están diseñados para optimizar el emplazamiento visual y comercial del producto. El empleo de estos planogramas es una forma de manipulación porque los investigadores han estudiado cómo piensa y compra la gente. Este conocimiento les sirvió para desarrollar mecanismos de control del impacto visual para aumentar el deseo de comprar de los consumidores.

Existe software y compañías enteras dedicadas a planificar y ejecutar estos planogramas para maximizar el efecto de mantener a los consumidores comprando.

Se emplean tres tipos de distribuciones para manipular a los consumidores:

- **Emplazamiento horizontal del producto:** Para aumentar la concentración del consumidor sobre cierto producto, se aplica un emplazamiento horizontal múltiple de un producto, uno al lado del otro. Algunos minoristas han comprobado que es necesario un emplazamiento mínimo de entre 15 y 30 centímetros del mismo producto para conseguir aumentar la atención del consumidor (véase la figura 6.8).

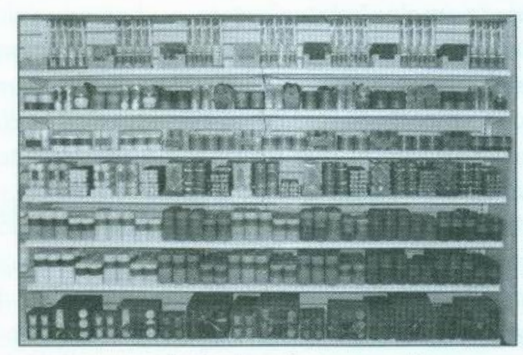


Figura 6.8. *Colocar productos iguales o parecidos en una fila horizontal, como se muestra en este planograma generado por ordenador, aumenta la atención del consumidor.*

- **Emplazamiento vertical del producto:** En este caso, un mismo producto se coloca en los distintos estantes, uno encima del otro hasta cubrir un espacio de entre 15 y 30 centímetros (véase la figura 6.9).

- **Emplazamiento por bloques:** Los productos que tienen algo en común se agrupan en bloques (marcas). Se pueden colocar unos al lado de otros o encima unos de otros, centrados o utilizando colgadores magnéticos (véase la figura 6.10).

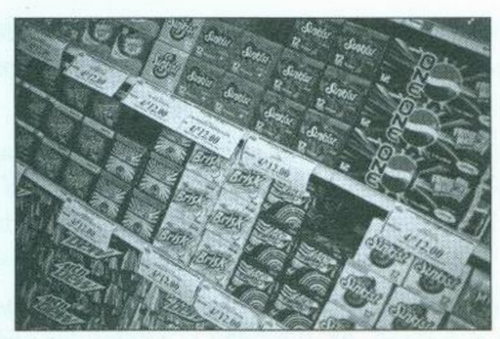


Figura 6.9. *Los productos se agrupan para captar la atención sobre lo que se quiere vender.*

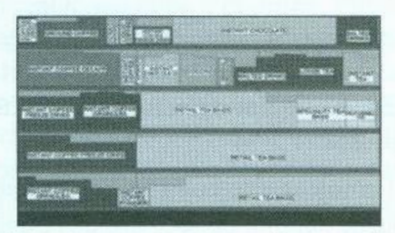


Figura 6.10. *Otro planograma generado por ordenador muestra la colocación en bloques.*

Los planogramas no son el único método para manipular a los consumidores. Se realizó una prueba en la que en un centro comercial sonaban bucles musicales diseñados específicamente. Los resultados mostraron que los consumidores permanecieron en el centro comercial una media de un 18 por 100 más de tiempo que cuando no sonaba la música. En la revista *Journal of Business Research*, Jean-Charles Chebat y Richard Michon publicaron un estudio que realizaron en un centro comercial de Canadá (`www.ryerson.ca/~rmichon/Publications/Ambient%20odors.pdf`).

Los investigadores perfumaron el aire con unos aromas especiales que supuestamente provocarían felicidad y ganas de comprar. El resultado fue que en la semana del estudio hubo un gasto medio de 50 euros más por consumidor. Sus visitas a la tiendas y a los centros comerciales ya nunca serán iguales.

No obstante, puede aprender mucho de estos métodos y experimentos. Saber cómo la gente agrupa las cosas en su cerebro puede ayudarle a organizarse para, de este modo, manipular los sentimientos, las sensaciones y los pensamientos de sus objetivos.

En lo que se refiere a los colores, existen muchas formas de manipular las emociones de un objetivo. En este campo se aplican muchos de los principios del emplazamiento de los productos. Los colores que elige para vestirse pueden

afectar a su objetivo. A continuación, elaboramos una pequeña lista con las formas en que un color concreto puede afectar el pensamiento o las emociones de otra persona:

- **Blanco:** El blanco normalmente se asocia con la pureza, la luz y la claridad. Provoca sentimientos de seguridad y neutralidad, así como de bondad y fe. Por este motivo, el blanco es utilizado en las bodas y como signo de rendición.
- **Negro:** El negro denota poder, elegancia, misterio y fuerza. Se emplea para indicar autoridad, profundidad y estabilidad. El negro provoca un sentimiento de calma y tranquilidad. También puede utilizarse para realzar otros colores.
- **Rojo:** El rojo se asocia con la excitación y la alegría. Denota celebración, acción y energía. Puede indicar buena salud, velocidad, pasión, deseo y amor. El rojo puede estimular emociones e incrementar el ritmo cardiaco y la presión sanguínea.

  Tenga cuidado al emplear este color: el rojo puede desatar emociones intensas. Aunque puede denotar poder e impulsividad, también indica fuerza, intimidación y conquista, incluso violencia y venganza. Tenga esto en cuenta cuando utilice este color.
- **Naranja:** El color naranja sugiere calidez, entusiasmo, atracción, determinación, fuerza y resistencia. Puede estimular a una persona para sentirse revitalizado e incluso desatar su apetito, pero debe tener cuidado, aunque puede reportar beneficios, como que el objetivo se sienta atraído y acogido por usted o su producto, en exceso o en una combinación equivocada puede provocar sentimientos de inseguridad, ignorancia y pereza.
- **Dorado:** Este color se asocia normalmente con la iluminación, la sabiduría, la riqueza y el prestigio.
- **Amarillo:** El color amarillo sugiere energía y optimismo, alegría, lealtad y frescura. Puede conseguir que el objetivo se centre y preste toda su atención.

  El amarillo también afecta a la memoria (¿por qué son amarillos los tacos de papel de notas autoadhesivos?). En pequeñas cantidades, puede desatar emociones positivas, pero en exceso puede provocar que el objetivo se desconcentre o se sienta criticado.
- **Verde:** Este color se asocia normalmente a la naturaleza, la armonía, la vida, la fertilidad, la ambición, la protección y la paz. Puede producir un efecto muy relajante, logrando que el objetivo se sienta a salvo.

- **Azul:** El azul es el color del cielo y el océano. Puede asociarse con la inteligencia, la intuición, la sinceridad, la tranquilidad, la salud, el poder y la sabiduría. Es muy relajante y refrescante y se sabe que ralentiza el metabolismo.

  El azul es el color en el que más fácilmente se pueden centrar los ojos. Puede tener muchos efectos positivos, pero asegúrese de no provocar que su objetivo sienta frío o cierto grado de hundimiento.
- **Morado:** Este color se asocia con la realeza, la nobleza, el lujo, la creatividad y el misterio.
- **Marrón:** El color marrón se relaciona con la tierra, la fiabilidad, la accesibilidad, los convencionalismos y el orden. Puede provocar sensación de arraigo o conexión o de poseer cierto sentido del orden.

¿Cómo puede emplear toda esta información? No estoy sugiriendo que simplemente vistiendo un traje azul va a conseguir que alguien se sienta lo suficientemente relajado como para entregarle una contraseña. Aun así, puede utilizar esta información para planificar sus vectores de ataque, asegurándose de maximizar sus opciones de tener éxito, incluyendo su aspecto y su manera de vestir.

Un ingeniero social debe analizar al objetivo que va a visitar para asegurarse de que la elección de colores que haga ayudará a manipularlo y no le desmotivará.

Por ejemplo, sabiendo que el color verde despierta sentimientos de avaricia o ambición, no lo empleará para acudir a un evento de una obra de caridad.

Por otro lado, visitar un despacho de abogados vistiendo de azul puede tener un efecto relajante que logre que el abogado se muestre más abierto. Planificar con cuidado estas tácticas y emplearlas con sensibilidad le ayudará a tener éxito en sus auditorías.

Condicionar al objetivo para que responda positivamente

El condicionamiento se utiliza en cualquier situación, desde una conversación normal al marketing o a la manipulación malintencionada. Al igual que el perro de Pavlov, la gente ha sido condicionada a responder a ciertos estímulos. La naturaleza humana se utiliza a menudo para manipular a la mayoría de las personas para que realicen las acciones que los manipuladores desean.

La mayoría de la gente cuando piensa en bebés sonríe, le resultan "monos" los animales que hablan y puede incluso ser manipulada para tararear la canción publicitaria de un producto.

Estas tácticas son tan encubiertas que en ocasiones ni siquiera sabemos si están funcionando. Muchas veces me pregunto qué tiene que ver una mujer en bikini con la cerveza.

Un ejemplo de la utilización del condicionamiento lo encontramos en los neumáticos Michelin (véase la figura 6.11). Durante años, esta empresa ha utilizado bebés en sus anuncios. ¿Por qué? "Porque hay mucho viajando sobre sus neumáticos". Pero estos anuncios esconden algo más. Al ver a un bebé, sonríe y se siente alegre. Esa emoción desata una reacción positiva que le condiciona a estar más dispuesto a aceptar lo que se le cuenta después. Cuando ve el bebé sonríe; cuando lo ve las veces suficientes está condicionado a experimentar sentimientos de calidez y alegría cuando ve los neumáticos Michelin.



Figura 6.11. *¿Verdad que son monos los bebés?*

Al ver al bebé junto al neumático identifica los sentimientos felices y positivos con esa marca. Éste es un ejemplo típico de manipulación.

Otro anuncio (véase la figura 6.12) que ha podido desconcertar a la gente es uno de la marca de cerveza Budweiser en el que aparecen unas ranas croando los sonidos "Bud", "weis" y "er". ¿Qué tienen que ver las ranas con la cerveza? En ese mismo sentido, encontramos la campaña de Clydesdale con un caballo y su pandilla de amigos animales. Estos anuncios son llamativos, incluso graciosos las primeras veces que los ve, pero en el fondo no puede explicar por qué consiguen que quiera comprar su cerveza.

El condicionamiento es una forma de manipulación muy sutil. Se ríe viendo el anuncio y después entra en la tienda, ve un cartel con las ranas o con el caballo y sonríe, creando un sentimiento positivo que le hace sentirse bien comprando ese producto.



Figura 6.12. Ranas vendiendo cerveza.

Estas tácticas se emplean a menudo en el mundo de las ventas y del marketing con la meta de manipular al consumidor para que compre los productos de la empresa en lugar de los de la competencia. Los ingenieros sociales no venden un producto, pero quieren que el objetivo les "compre" lo que les están vendiendo: el pretexto que presentan y las acciones que quieren que realice el objetivo. Pero, ¿por qué emplear la manipulación? ¿Cuáles son los incentivos para utilizar esta poderosa forma de control? En la siguiente sección se explica este punto.

Incentivos de la manipulación

¿Cuáles son los incentivos de manipular a alguien? Esta pregunta llega hasta las raíces de los métodos, el pensamiento y las tácticas empleadas en la manipulación. No toda manipulación es negativa, pero siempre está relacionada con los incentivos que se esconden detrás. Y cada "incentivo" puede ser positivo o negativo.

¿Qué es un incentivo? Un incentivo es cualquier cosa que le motiva a realizar cierta acción. Puede ser dinero, amor, éxito; cualquier cosa, incluidas las emociones negativas como el odio, los celos o la envidia. Las razones principales por las que las personas eligen manipular a otros pueden dividirse en tres categorías: económicas, sociales e ideológicas. Las siguientes secciones explican cada uno de estos tipos de incentivo y cómo aplicarlos a la manipulación.

Incentivos económicos

Este tipo de incentivos suelen ser los más habituales, como en los casos mencionados previamente relacionados con el aumento de las ventas. Muchas estafas esconden detrás un incentivo económico.

¿Cuánta gente juega a la lotería cada día con la esperanza de ganar el sorteo? Puede llegar a gastar cientos de euros con el tiempo y el hecho de ganar un reintegro de 20 euros es suficiente para hacerle feliz y que quiera continuar jugando. Un ejemplo no malintencionado de incentivo económico son los cupones de descuento. Si compra este producto específico en esta tienda concreta, obtendrá X euros de descuento. Si es un comprador ahorrativo o quiere probar ese producto, acudirá a esa tienda. Muchos anuncios que le animan a ampliar su educación, su carrera o habilidades profesionales usan estos incentivos presentándole el panorama de que sus ingresos aumentarán después de que realice el curso que le ofrecen.

El incentivo para emplear la manipulación en los ataques maliciosos es el beneficio económico propio y, por lo tanto, su motivación y su técnica reflejan este hecho. Por ejemplo, si la meta del ingeniero social malicioso es que el objetivo le entregue parte del dinero que tanto le ha costado ganar, utilizará pretextos a los que se les "permita" pedir ese dinero: pretextos como obras de caridad encajan con este escenario, porque en estos casos es normal pedir donaciones o información financiera.

Incentivos ideológicos

Los incentivos ideológicos son los más difíciles de describir. Los ideales de cada persona son diferentes y afectan al incentivo. Si su sueño en la vida es montar un restaurante, entonces ésa es su pasión. Trabajará más horas y dedicará más esfuerzo que el resto de sus empleados. También trabajará por menos dinero, porque será su sueño y su motivación; para el resto de personas, sólo será un trabajo. Los sueños y las creencias pueden estar tan integrados en una persona que separarlos de ella llegue a ser casi imposible. ¿Cuándo escucha la frase "tengo un sueño", piensa en Martin Luther King? Los sueños y las metas de algunas personas son quiénes son, no lo que piensan.

La gente tiende a unirse a otras personas con sueños y metas parecidas, por este motivo el refrán "Dios los cría y ellos se juntan" es relevante en esta explicación. Pero éste también es el motivo por el que tantas personas pueden ser manipuladas.

Piense en los telepredicadores cristianos, por ejemplo. Las personas que tienen fe y un deseo de creer en Dios se agrupan a su alrededor. Personas de ideas afines pueden reforzar la fe y el deseo de hacer lo correcto los unos a los otros, pero el

telepredicador puede emplear esa ideología para convencerles de que el deseo de Dios es que esa iglesia particular prospere, llenando de paso de billetes los bolsillos del telepredicador.

El telepredicador da unos cuantos sermones motivadores, derrama algunas lágrimas y de pronto la gente le está entregando cheques. Los telepredicadores emplean las herramientas tanto de los ideales económicos como de los sociales (vea la siguiente sección, "Incentivos sociales") para transformar los ideales de la audiencia y conseguir que entreguen su dinero. Lo más interesante es que si le pregunta a un seguidor qué piensa de que el predicador sea mucho más rico que él, afirmará que es la voluntad de Dios. Sus ideales han sido transformados o manipulados.

Los incentivos ideológicos también se pueden utilizar para bien, por ejemplo educando a la gente sobre su moral y ética, y también puede ser muy efectivo recurrir a emplear el miedo como incentivo. Los incentivos ideológicos suelen enseñarse a los niños a través de cuentos y fábulas que tienen un sentido oculto. Los hermanos Grimm son un gran ejemplo de este incentivo. Los cuentos en que los personajes malvados acaban sufriendo dolor físico o incluso la muerte y los buenos superan todo tipo de dificultades obteniendo una gran recompensa al final refuerzan a través del miedo la idea de que ser malo conduce a la muerte o a un castigo terrible.

Los incentivos ideológicos también se emplean en el marketing emplazando anuncios donde los ideales afines convergen. Por ejemplo, los fabricantes de pañales se anuncian en revistas familiares, los refugios para animales abandonados se anuncian en el zoo, las marcas de ropa deportiva se anuncian en eventos deportivos, etc. Este tipo de incentivo aumenta las posibilidades de que las personas que comparten los mismos ideales compren los bienes o servicios anunciados. Este incentivo se emplea para alinear los ideales propios con los de otras personas afines. A menudo, cuando una persona se siente atraída hacia una causa, es cuando empieza la manipulación. Lo volvemos a decir, no toda la manipulación es mala, pero hay que saber emplearla del modo correcto.

Incentivos sociales

Probablemente, los incentivos sociales son los que más ampliamente se utilizan, especialmente en ingeniería social.

Los humanos somos seres sociales por naturaleza; eso es lo que hacemos en nuestra vida diaria. Además, los incentivos sociales engloban todos los demás tipos de incentivo. Una relación adecuada puede mejorar su situación económica y puede también ajustar, alinear o ampliar sus ideales. Puede decirse que los incentivos sociales son más fuertes que los otros dos tipos de incentivos.

Es fácil observar el poder que tiene la presión de grupo sobre muchas personas. Tanto para los mayores como para los jóvenes, la atracción de la conformidad es poderosa. Muchas veces lo que se considera aceptable está conectado con un incentivo social. El concepto que tenemos de la vida y de nosotros mismos puede estar muy afectado por nuestro entorno social. Básicamente, la presión de grupo puede existir incluso sin que exista el propio grupo.

¿Soy una persona guapa? Bueno, eso depende. Si estoy en Estados Unidos donde las supermodelos utilizan la talla cero y los hombres tienen músculos en sitios donde ni siquiera sabía que existen, probablemente no. Si soy un ciudadano de la antigua Roma, donde ser más grande indica poder y riqueza, entonces puede que sí. Nuestro fuero interno se ve influenciado por nuestra visión del mundo.

En 1975 la fuerza aérea estadounidense condujo un estudio titulado "Identification and Analysis of Social Incentives in Air Force Technical Training" (Identificación y análisis de los incentivos sociales en el entrenamiento técnico de las fuerzas aéreas), para intentar comprobar el poder de los incentivos sociales para formar líderes durante las sesiones de entrenamiento. Se condujeron cuatro escenarios diferentes con un grupo y se analizaron los efectos que habían tenido sobre los estudiantes.

El resultado final fue que un incentivo social concreto, normalmente relacionado con los elogios o el refuerzo positivo de los compañeros o los superiores, creó un fuerte vínculo entre los estudiantes y los instructores:

La conclusión más importante de esta investigación es que el manejo de los incentivos sociales es un arte especialmente complicado. Aunque los incentivos sociales son relativamente sencillos de identificar y clasificar, la manipulación y manejo de esos mismos incentivos requieren un esfuerzo bastante mayor. La información escalonada mostró un alto valor de varios incentivos sociales. Los resultados del experimento de campo mostraron la positiva influencia del ejercicio de reconocimiento y contracción psicológica en actitudes hacia los compañeros. Estos dos descubrimientos subrayan la importancia de los factores sociales.

En otras palabras, aumentar o reducir el atractivo del incentivo social no es demasiado difícil una vez que sepa lo que motiva a la persona. Este fenómeno es especialmente evidente en los grupos de adolescentes. Cuando descubren lo que molesta a alguien, lo utilizan como arma para forzar su docilidad. Cuanto más grande sea el grupo que hace la presión, más probabilidades tendrá de que el objetivo ceda.

Ésta es una afirmación importante. Me pregunto cuál habría sido el resultado de esta investigación si los investigadores hubieran podido utilizar la cantidad de sitios Web de medios sociales que existen hoy en día. La presión de grupo es una influencia muy fuerte, todo el mundo quiere encajar y formar parte.

Los incentivos sociales funcionan. En 2007, un grupo de investigadores (Oriana Bandiera, Iwan Barankay e Imran Rasul) escribieron un artículo titulado "Social Incentives: The Causes and Consequences of Social Networks in the Workplace" (Los incentivos sociales: causas y consecuencias de las redes sociales en el lugar de trabajo): `www.social-engineer.org/wiki/archives/Manipulation/Manipulation-Social-Incentivespdf.pdf`.

El informe es un estudio interesante en la línea del estudio de las Fuerzas Armadas, pero realizado en 2007. La investigación analiza cómo las personas que tienen "amigos" en el trabajo realizan su labor cuando trabajan en grupo con esos amigos. Su conclusión:

Nuestros descubrimientos indican que existen incentivos sociales: la presencia de amigos afecta la productividad del trabajador, a pesar de la ausencia de externalidades de esfuerzo laboral sobre los compañeros debido a la producción tecnológica o al sistema de compensación en su lugar. Debido a los incentivos sociales, los trabajadores se ajustan a una norma común cuando trabajan juntos. El poder de la norma es tal, que la presencia de amigos eleva la productividad de los trabajadores menos capaces y reduce la productividad de los trabajadores más capaces.

Los incentivos sociales son un determinante cuantitativo importante del rendimiento de un trabajador. Ya que los trabajadores reciben un pago a destajo basado en la productividad individual, la fuerza de los incentivos sociales es tal que (i) los trabajadores más capaces están dispuestos a renunciar al 10 por 100 de sus ganancias con tal de ajustarse a la norma; (ii) los trabajadores que tienen al menos un amigo más capaz que ellos mismos están dispuestos a aumentar su productividad en un 10 por 100 para cumplir con la norma. En conjunto, la distribución de la capacidad de los trabajadores es tal que el efecto último domina de manera que el efecto neto de los incentivos sociales sobre el rendimiento es positivo.

La presencia de amigos implica que la persona trabajará más o menos dependiendo de su nivel de trabajo normal. La presión de grupo en ausencia de presión real puede afectar al trabajo de la gente. La presión se percibe según lo que se considera normal. ¿Por qué? Quizá, aunque una persona pueda trabajar mejor o más rápido no quiere parecer un sabelotodo o un "pelota", como a veces se denomina a esta gente. Quizá, si normalmente es un holgazán, no quiere que lo consideren un vago y se esfuerza un poco más. En ambos casos, su ética del trabajo se ve afectada por sus amigos.

Una buena táctica de gerencia es poner siempre a los mejores trabajadores y los líderes naturales por encima. Pero hay mucho que aprender de esta investigación. Éste es un método muy utilizado por los ingenieros sociales. Al unirse a un gran grupo de gente que vuelve a la oficina después del almuerzo y parecer uno de los empleados, las opciones de ser descubierto por el guardia al cruzar la puerta se

minimizan. También es la forma en que se puede manipular a un grupo para que piense que cierta acción o actitud es aceptable. Puede comprobar este hecho en la industria del entretenimiento, donde parece que cada año el estándar de lo que es moralmente aceptable desciende un poco más, vendiéndose esta caída como "libertad".

Estos tres tipos incentivos no son los únicos que se utilizan. Pueden derivar en otros aspectos que escapan al alcance de este libro, pero aún se mantiene la cuestión de cómo emplearlos en ingeniería social.

La manipulación en ingeniería social

La manipulación consiste menos en lograr que los demás piensen como usted o se sientan cómodos y más en coaccionarlos para que hagan lo que desea. La palabra "coacción" no es muy agradable. Significa "forzar para pensar o actuar de cierta manera" o "dominar, contener o controlar por la fuerza".

La manipulación y la coacción emplean la fuerza psicológica para alterar la ideología, creencias, actitudes o conductas del objetivo. La clave es aplicarlas con pasos tan pequeños que sean casi imperceptibles. El ingeniero social no debe alertar al objetivo de que está siendo manipulado. Algunos de los siguientes métodos pueden resultar controvertidos o absolutamente horribles, pero se utilizan a diario por estafadores, ladrones de identidad, etc. Una de las metas de la manipulación puede consistir en provocar ansiedad, estrés y un exceso de presión social. Cuando el objetivo se siente de ese modo es más sencillo que realice la acción que el ingeniero social desea.

Teniendo esto en cuenta, puede comprender por qué normalmente se piensa en la manipulación en términos negativos, pero se emplea en ingeniería social y, por tanto, debemos abordarla.

Aumentar la sugestibilidad del objetivo

Aumentar la sugestibilidad del objetivo puede implicar la utilización de la programación neurolingüística (PNL) explicada en el capítulo 5 u otras pistas visuales. Previamente, ha visto cómo se puede condicionar a una persona con el clic de un bolígrafo u otros ruidos o gestos que pueden provocar emoción, incluso sin utilizar las palabras.

Pude ver este principio en acción en una ocasión en la que estaba con un individuo que manipulaba a un objetivo. Hacía clic con el bolígrafo una vez para indicar un pensamiento positivo. Decía algo positivo, sonreía y hacía clic con el bolígrafo. Comprobé cómo el objetivo empezaba a sonreír cada vez que escuchaba el clic del

bolígrafo. Entonces, la persona con la que estaba inició una conversación sobre un asunto muy deprimente pero hizo clic con su bolígrafo y el objetivo sonrió e inmediatamente se sintió avergonzado. Ese sentimiento era lo que necesitaba para manipular al objetivo para que hiciera lo que deseaba.

Una situación en la que la otra persona se sienta susceptible a la sugestión se puede crear a través de la repetición de ideas u otros métodos que consigan que el objetivo acepte las ideas que se le presentan. Debe asegurarse de que todos los detalles vayan en la dirección de esta manipulación: las frases utilizadas, las imágenes que evocan las palabras, la elección de colores: Todo esto hará más susceptible al objetivo.

William Sargant, un polémico psiquiatra autor del libro *La conquista de la mente humana*, habla de los métodos a través de los cuales la gente es manipulada. Según Sargant, se pueden implantar varios tipos de creencias en el objetivo una vez que ha sido perturbado con miedo, ira o excitación. Estos sentimientos causan una sugestibilidad intensificada y deficiencias en el juicio.

Un ingeniero social puede aprovechar este fenómeno ofreciendo al objetivo una sugerencia que le provoque miedo o excitación para ofrecer después una solución que se transforma en una sugestión. Por ejemplo, en el programa de la cadena de televisión BBC, *The Real Hustle*, prepararon un timo para demostrar cómo funciona este concepto, en el cual montaban un puesto en un centro comercial en el que se podían comprar billetes para una rifa. La gente compraba un billete a cambio de la oportunidad de ganar tres premios de mucho más valor que el precio del billete.

Una mujer compró un billete y, por supuesto, ganó el mejor premio. Estaba muy excitada porque nunca había ganado nada parecido. En ese momento, Paul Wilson realizó la sugestión para manipularla: en el punto álgido de su excitación le dijo a la señora que tenía que llamar a un número de teléfono y dar los datos de su cuenta bancaria para reclamar el premio. Lo hizo sin pensarlo dos veces. La sugestión tenía sentido para ella, sobre todo en ese momento especial.

Conocer al objetivo y sus gustos, el nombre de sus hijos, sus equipos favoritos y su comida preferida y utilizar estos datos para crear un ambiente emocional hará mucho más fácil la existencia de una atmósfera susceptible.

Controlar el entorno del objetivo

El control del entorno del objetivo se emplea a menudo en la ingeniería social *on-line*, las estafas y el robo de identidad. Al entrar a formar parte de las mismas redes sociales que el objetivo, el atacante consigue el tiempo necesario para establecer contacto y manipularlo para que actúe o piense como desea. Las redes sociales también se pueden utilizar para descubrir cuáles son las cosas que motivan al objetivo.

Utilicé este método en una ocasión en la que buscaba a un estafador para un cliente que quería sus detalles de contacto. Conseguí abrir una cuenta en un foro en el que solía contar sus "logros". Empleando esta táctica de introducirme en su entorno y entablar una amistad con él, conseguí ganarme su confianza y utilizar sus redes sociales para saber lo que estaba haciendo para, finalmente, conseguir sus datos de contacto.

En esta técnica de manipulación, se puede emplear cualquier método para controlar el entorno del objetivo. Esto puede ser tan sencillo como abordarlo cuando sabe que no le interrumpe o permitir o evitar que el objetivo vea algo para provocar una reacción.

Por supuesto, a no ser que pretenda encerrar al objetivo en un armario, es imposible controlar todo su entorno y controlar tanto como pueda conlleva planificación e investigación. Después de localizar los círculos sociales del objetivo, ya sea *on-line* o en el mundo real, debe planificar cómo entrar en ellos y controlar ese entorno.

Una vez dentro, ¿qué elementos quiere controlar? Un buen ingeniero social se tomará tiempo para construir una relación y reunir información antes de dar el golpe final.

El control del entorno se emplea a menudo en los interrogatorios de la policía o en tiempo de guerra. El entorno en el que se realiza el interrogatorio creará una atmósfera en la que el objetivo se sienta cómodo, nervioso, intimidado, ansioso o en cualquier otro estado en el que se desee que se encuentre.

Forzar al objetivo a revaluar

Socavar las creencias, la conciencia o el control emocional de una situación del objetivo tiene un efecto desestabilizador en él. Ésta es una táctica muy negativa porque se emplea para hacer dudar al objetivo de las cosas que considera ciertas.

Las sectas utilizan esta táctica para aprovecharse de aquéllos que buscan dirección en la vida. En muchas ocasiones, la gente que se siente perdida o confundida está convencida de que todo su sistema de creencias necesita revaluarse. Cuando la secta toma el control, puede llegar a convencer a las víctimas de que sus familiares y amigos no saben lo que es mejor para ellas.

En el campo de la ingeniería social, puede lograr que una persona revalúe las creencias que tiene sobre lo que es seguro y lo que es inseguro o sobre lo que es política de empresa y lo que no lo es. A diario se emplean tácticas similares presentando un argumento bien pensado que provoque que el objetivo revalúe su posición en cierto tema y le haga dudar. Por ejemplo, en la economía

actual, los vendedores están ansiosos por vender. Puede llamar al departamento de ventas de una empresa que tenga unas políticas estrictas en relación con las descargas de archivos PDF sin las adecuadas medidas de precaución y puede decir lo siguiente:

"Hola, soy de la compañía X y quería hacer un pedido de 10.000 unidades de su producto. Necesitamos tres presupuestos para ver cuál es el mejor. He subido la información a nuestro sitio Web; ¿puedo darle la URL? Tengo una reunión en dos horas. ¿Puede echarle un vistazo y darme un presupuesto preliminar antes de que me vaya?".

¿Cree que esta táctica puede funcionar? Lo más probable es que el vendedor descargue y ejecute el archivo sin pensarlo demasiado. Ha logrado que revalúe las políticas que le han enseñado.

Lograr que el objetivo se sienta impotente

Conseguir que el objetivo se sienta vulnerable o impotente es otra táctica siniestra pero muy efectiva. Se emplea a menudo en ingeniería social cuando el pretexto es un ejecutivo enfadado o alguien que tiene poder sobre el objetivo. Enfadado por la falta de respuestas o por la incapacidad del objetivo para contestar con rapidez, el atacante le reprende o amenaza, haciendo que dude de su posición y sienta que no tiene poder sobre la situación.

Otro método más sutil consiste en socavar el sistema de creencias empleando incentivos sociales. En una auditoría, me detuvo un conserje mientras escaneaba unos documentos. Hizo lo correcto pero yo reaccioné diciendo algo como: "¿Sabías que cada año esta empresa mantiene una lucha constante para evitar los ataques a través de la red? ¡Estoy intentando que esta empresa sea más segura y tú no me permites hacer mi trabajo!". Mi comportamiento apabullante hizo que se sintiera muy impotente y por lo tanto retrocedió.

Darle al objetivo la impresión de que no tiene tiempo para pensar o que la situación es urgente también puede hacerle sentir impotente. No puede tomarse tiempo para pensar cómo manejar el problema y, por tanto, debe tomar una decisión de una forma que sabe que no es la correcta.

Esta táctica se utilizó después de los recientes terremotos de Haití. Se lanzó un sito Web que afirmaba tener información sobre personas desaparecidas. Como, según ellos, nadie más podía facilitar esta información, podían permitirse ciertas exigencias.

Mucha gente desesperada e impotente facilitó mucha información y entró en muchos lugares de Internet en los que sabían que no deberían haber entrado, viéndose dañados por ello en última instancia.

La BBC publicó una historia hablando de este tema y elaboró una larga lista de consejos para poder permanecer protegido: `http://news.bbc.co.uk/2/hi/Business/8469885.stm`.

Infligir castigo no físico

Íntimamente conectado con hacer sentir impotente al objetivo está hacerle sentir culpable, humillado, ansioso o desfavorecido. Estos sentimientos pueden ser tan fuertes que el objetivo llegue a hacer cualquier cosa por volverse a ganar su "favor". La culpa por no haber cumplido con las expectativas puede causar humillación y duda, lo que puede provocar que el objetivo reaccione como quiere el atacante.

No estoy sugiriendo que se utilice la humillación de forma constante, pero he visto cómo se utilizaba en una ocasión para abrir a un objetivo y en otra situación para ablandarlo y hacerlo más maleable y vulnerable a la sugestión.

El primer atacante se acercó al objetivo en un lugar público para intentar obtener una información; representaba el papel de alguien importante.

En mitad de la conversación aparece una subordinada (cómplice en el plan) y hace una pregunta que enfada mucho al primer atacante. Reacciona diciendo: "Debes de ser la persona más estúpida que conozco". En un ataque de ira, se marcha. La otra atacante da muestras de estar muy dolida y abatida y es consolada inmediatamente por el objetivo. La empatía del objetivo hace que le puedan manipular para revelar mucha más información de la que hubiera deseado.

Intimidar a un objetivo

La intimidación no debe emplearse de modo habitual en ingeniería social. No va a atar al objetivo y actuar con él como un matón, pero puede utilizar la intimidación de maneras más sutiles.

Sugerir que si no accede a lo que pide puede conllevar que le despidan u otras consecuencias negativas puede intimidar al objetivo haciéndole reaccionar. Los gobiernos emplean esta táctica muy a menudo para manipular a la sociedad para que crea que el sistema económico se viene abajo. De esta forma, puede controlar las emociones de la gente.

Una forma de emplear esta táctica es sencillamente mostrar una apariencia intimidante. Parecer ocupado, disgustado o enfrascado en una tarea importante puede intimidar a mucha gente. Hablar con un aire autoritario también funciona.

En los negocios, enviar documentos por correo certificado o por mensajero conlleva cierto nivel de intimidación. Hacer que la persona tenga que firmar al recibir un paquete de contenido incierto puede conseguir que algunas personas

se sientan intimidadas en cierto modo. La meta con esta táctica es lograr que el objetivo se sienta incómodo y ansioso, lo que hará que reaccione de un modo del que luego se pueda arrepentir.

Muchos ingenieros sociales y auditores profesionales utilizan estas técnicas siniestras de manipulación con mucho éxito. Cuando una persona ha sido manipulada para sentirse indefensa, es más probable que se rinda ante el atacante.

Aquí es donde existen ciertas diferencias entre la manipulación en ingeniería social y en otras formas de influencia. En la manipulación negativa, el atacante desaparece sin importarle cómo se siente el objetivo después. Aunque el objetivo se percate de lo que ha sucedido, ya es demasiado tarde porque el daño ya está hecho. Existen otros aspectos de la manipulación igual de poderosos pero menos siniestros.

Emplear la manipulación positiva

La manipulación positiva tiene las mismas metas que la negativa: al final el objetivo está alineado con los pensamientos y deseos del atacante. Las diferencias están en la forma de llegar a ese punto. En la manipulación positiva, el objetivo no necesita recurrir a la terapia cuando todo ha terminado.

En mis años de investigación he reunido algunas notas sobre el modo en que los padres interactúan con sus hijos para lograr que hagan lo que los padres desean. A menudo, se emplean técnicas de manipulación positiva que pueden ser útiles en ingeniería social.

Desconecte su emoción de la conducta del objetivo

Es importante mantener sus emociones separadas de la conducta del objetivo. En el momento en que permite que sus emociones se involucren, el objetivo le está manipulando. Puede sentir emociones, por supuesto, pero controle lo que siente y cómo demuestra ese sentimiento. No debe perder el control. También debe controlar las emociones negativas todo lo posible.

Al desconectar sus emociones puede lograr que la gente se sienta cómoda. Esto no significa que no muestre emoción alguna; eso resulta molesto a los demás. Si alguien se siente disgustado, es bueno mostrar la cantidad adecuada de preocupación pero si se excede en su demostración puede descolocar al objetivo arruinando la acción. Mantenga sus emociones alineadas con su pretexto. Si no permite que sus emociones se impliquen mantendrá el control en todo momento. Un buen ingeniero social es capaz de hacerlo a pesar de las actitudes o acciones del objetivo. Si el objetivo está disgustado o enfadado o se muestra beligerante o maleducado, el ingeniero social se mantiene tranquilo y atento.

Intente mencionar las cosas positivas

Siempre que pueda, intente bromear sobre algo o hacer un cumplido, pero sin resultar repulsivo. No debe acercarse a un guardia de seguridad y decir: "Esto son dos monjas que entran en un bar...". Este método puede ser desastroso. Del mismo modo, no puede entrar en una oficina y decirle a la chica del mostrador: "Vaya, qué guapa eres". Encontrar algo positivo que decir hace que la gente se sienta cómoda pero debe hacerse con control y buen gusto. Utilizando el ejemplo de abordar a un guardia de seguridad, después de presentarse, puede decir algo positivo sobre la foto de su hija: "Vaya, que niña más mona; ¿cuántos años tiene? Yo también tengo una hija pequeña".

Presuponer, presuponer y presuponer

Probablemente, habrá oído lo que dicen sobre la gente que da las cosas por sentadas, pero en este caso, "dé todo por hecho". Dé por hecho que el objetivo va a actuar como usted quiere, dé por hecho que va a responder como desea y que va a acceder a todas sus peticiones.

Dé las cosas por sentadas con sus afirmaciones y con sus preguntas: "Cuando vuelva del cuarto de servidores...". Esta afirmación presupone que pertenece a ese lugar y que ya tiene permiso para acceder. En la situación con el guardia de seguridad mencionada previamente, después del cumplido puede continuar diciendo: "Cuando vuelva de comprobar los servidores le enseñaré una foto de mi hija".

Presuponer que lo que quiere va a ocurrir también es un punto muy importante porque afecta a su perspectiva. Debe dar la impresión de que va a conseguir lo que ha venido a buscar; ese sistema de creencias afectará a su lenguaje corporal y a sus expresiones faciales ayudando a su pretexto para que funcione.

Si entra en acción pensando que va a fracasar, fracasará o, como mínimo, ese pensamiento afectará a su lenguaje corporal y expresiones faciales. Del mismo modo, si está convencido de que tendrá éxito, es más probable que así sea. Una advertencia: no llegue hasta el punto de resultar arrogante. Por ejemplo, pensar: "Esto lo tengo hecho porque soy increíble y soy el mejor", puede afectar a su conducta y provocar rechazo en su objetivo.

Pruebe distintas líneas

Lo normal es empezar con los típicos por qué/cómo/cuándo, pero intente otros métodos para ver qué sucede. El grupo de investigación que dirige un popular sitio Web de citas (`www.okcupid.com`) reunió unos datos que muestran el valor de empezar la interactuación de forma diferente y original.

¿Recuerda la discusión sobre los cumplidos? Los investigadores de OkCupid descubrieron que empezar una conversación con un cumplido exagerado tiene el efecto contrario al deseado. Palabras como "sexy", "preciosa" o "excitante" tienen efectos desastrosos, mientras que palabras como "maravilloso" o "fascinante" resultan más positivas. También llegaron a la conclusión de que saludar con expresiones como "hey" u "hola" desmotiva al objetivo mientras que expresiones como "¿cómo va eso?" o "¿qué tal estás?" funcionan muy bien.

Por supuesto, estas estadísticas son de un sitio Web de citas, pero la idea es que la gente reacciona mejor a los saludos originales. Del mismo modo, en una situación de ingeniería social, cambie su forma de presentarse y comprobará un cambio en la reacción de sus objetivos a su mensaje.

Utilice el tiempo pasado

Cuando quiera tratar un asunto negativo que no quiere que el objetivo repita, construya la frase en pasado. Esta técnica pone las actitudes y acciones negativas en el pasado en la mente, haciendo "borrón y cuenta nueva" para empezar a tratar asuntos positivos. Por ejemplo: "Cuando 'dijo' que no 'podía' pasar a ver al señor Smith..." en oposición a: "Cuando 'dices' que no 'puedo' pasar a ver al señor Smith...". Sólo ha cambiado el tiempo verbal, pero el efecto es muy importante. Da la impresión de que la afirmación negativa está lejos en el pasado y es el momento de avanzar a algo nuevo y positivo. También se consigue que el objetivo vea que usted lo considera ya en el pasado.

Localizar y destruir

Identifique, trace el mapa y planifique cómo va a manejar cualquier actitud negativa o perjudicial. Imagine que su pretexto es un técnico del servicio de asistencia que quiere acceder al cuarto del servidor. Sabe que todos los días a las diez de la mañana un grupo grande de empleados se toma un descanso para salir a fumar. Ha decidido que ése es un buen momento porque hay gente entrando y saliendo. Llega preparado pero, al entrar en el edificio, la recepcionista acaba de recibir una mala noticia y está emocionalmente aturdida. Debe tener un plan para solucionar este problema.

Si no piensa cómo manejar las potenciales barreras comunicativas o influencias negativas y espera a que sucedan para reaccionar, cuando ocurran seguramente no las manejará bien. Esto plantea una interesante reflexión. Debe sentarse y pensar como el objetivo: ¿Qué objeciones se pueden plantear? ¿Qué puede decir cuando se le acerca una persona que no conoce? ¿Cómo reaccionará? Pensar en este tipo de cosas puede ayudarle a diseñar un plan para manejar esos problemas.

Escriba sus ideas y las posibles objeciones del objetivo y simule el encuentro. Haga que su pareja interprete el papel del guardia de seguridad. Por supuesto, habrá cosas como las expresiones faciales que no se podrán imitar, pero puede utilizar una lista de barreras comunicativas para comprobar cómo responde a ellas.

Practique hasta que se sienta confiado y cómodo, pero no totalmente programado por un guión. Recuerde que su reacción no debe establecerse con tanta rigidez que no pueda variarla si fuera necesario. La manipulación positiva puede tener un efecto muy intenso en su objetivo. No sólo conseguirá que no se sienta violentado, si lo hace correctamente, el objetivo puede tener la sensación de haber hecho una buena acción.

Resumen

La manipulación es un componente clave de la ingeniería social y de la influencia. Este capítulo aborda áreas del comportamiento humano que abarcan años de investigación de algunas de las mentes más brillantes del planeta.

Algunas reacciones habituales a la idea de la manipulación pueden ser:

- "No quiero manipular a los demás".
- "Me siento mal por aprender estas cosas".

Estos comentarios representan la manera de pensar habitual de la gente cuando escucha la palabra "manipulación". Espero que ahora esté convencido de que la manipulación no siempre es un arte oscuro y puede utilizarse para bien.

El campo de la influencia ha sido diseccionado, investigado y analizado por algunos de los psicólogos e investigadores más brillantes de la actualidad. Esta investigación sirve como base para mi propia investigación para desarrollar la información de este capítulo.

La sección del encuadre, por ejemplo, puede cambiar realmente la forma en que interactúa con los demás y el concepto de la reciprocidad puede moldear su forma de pensar como ingeniero social y su manera de emplear la influencia. La influencia es un tema tan asombroso que existen volúmenes enteros dedicados sólo a ella.

Comprender lo que hace reaccionar a una persona para motivarla para que realice cierta acción y conseguir que esa persona considere que la acción es positiva para ella: ése es el poder de la influencia. Este capítulo aclara la ciencia y la psicología de la motivación de la gente y explica cómo utilizan la influencia los ingenieros sociales.

Recuerde: la influencia y el arte de la persuasión son los procesos para conseguir que alguien "quiera" actuar, reaccionar, pensar o creer del modo en que "usted" desea que lo haga.

El poder de esta afirmación trasciende los límites de este libro. Es la clave para alterar cualquier encuadre, la llave para abrir cualquier puerta y el camino para convertirse en un maestro de la persuasión.

Los ingenieros sociales también emplean muchas herramientas físicas, algunas de las cuales parecen sacadas de una película de James Bond. Las analizamos en el siguiente capítulo.

7. Las herramientas del ingeniero social

El hombre es un animal que necesita herramientas. Sin ellas no es nada, con ellas lo es todo.
Thomas Carlyle

Para tener éxito en ingeniería social, es fundamental contar con un buen juego de herramientas. Además, no se trata tan sólo de poseer las herramientas, sino de saber cómo utilizarlas en su trabajo.

Este capítulo explica las diferencias entre las herramientas físicas, las herramientas telefónicas y el software. Tenga en cuenta que el simple hecho de poseer las más caras o las mejores, no le convierte en un ingeniero social. Las herramientas pueden mejorar su práctica de seguridad del mismo modo en que la mezcla correcta de especias mejora una comida: es necesario emplear la cantidad adecuada. No es cuestión de que aparezca en una actuación de seguridad como Batman con un cinturón de herramientas repleto, pero tampoco debe encontrarse en la puerta de un objetivo sin el juego de herramientas adecuado para acceder.

Este capítulo podría ser interminable, pero no pretendo que este libro se convierta en un manual sobre cómo abrir cerraduras con ganzúas o interceptar números de teléfono. En lugar de eso, es un intento de ofrecerle la suficiente información para que decida qué herramientas pueden serle de utilidad en su práctica.

La primera sección del capítulo se centra en conceptos como las ganzúas, las cuñas y las cámaras. Han llegado al mercado nuevas herramientas que harán a cualquier ingeniero social sentirse como James Bond. Este capítulo explica cómo utilizar algunas de esas herramientas y muestra imágenes de ellas. Además, se proporciona información sobre cómo interceptar un teléfono en una auditoría, continúa con un repaso del mejor software de recopilación de información del mercado y termina explicando las herramientas de descifrado de contraseñas.

Herramientas físicas

La seguridad física son las medidas que toman las personas o las empresas para estar seguros que no implican la utilización de ordenadores. Normalmente, consisten en cerraduras, cámaras de vigilancia, sensores de movimiento, etc. Comprender la seguridad física y su funcionamiento es parte de la ingeniería social. No es necesario que sea un experto en estos dispositivos, pero comprender los mecanismos de seguridad que emplea el objetivo le ayudará a superar obstáculos que pueden aparecer en sus auditorías.

Ganzúas

Antes de explicar cómo abrir cerraduras, debe saber cómo funcionan.

La figura 7.1 muestra una imagen muy esquemática de una cerradura sencilla.

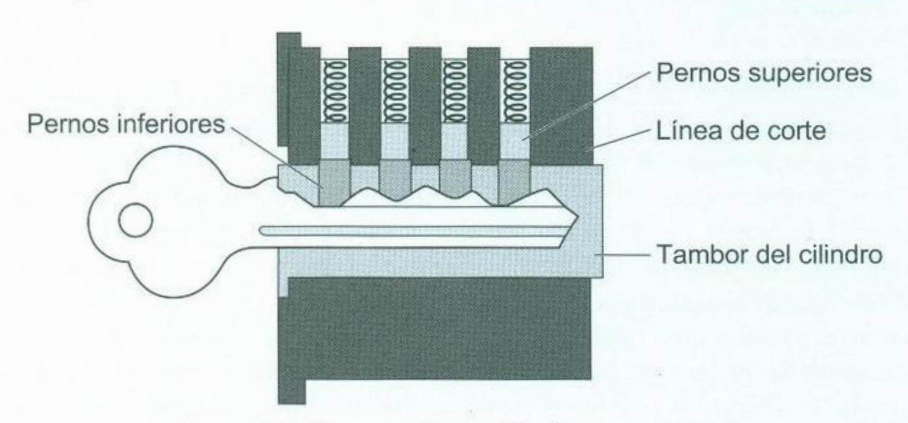


Figura 7.1. *Un esquema sencillo de una cerradura.*

Básicamente, el modo en que funciona una cerradura es mediante unos pernos accionados por la llave. La llave empuja hacia arriba los pernos y cuando éstos se alinean permiten que la llave gire abriendo la puerta.

Una ganzúa imita el funcionamiento de la llave, moviendo los pernos a su posición correcta uno a uno, permitiendo que la cerradura gire y la puerta se abra. Necesita dos herramientas para abrir una cerradura: las ganzúas y la herramienta de tensión.

Las ganzúas son piezas largas de metal curvadas en el extremo, parecidas a las herramientas de un dentista. Se introducen en la cerradura y mueven los pernos arriba y abajo hasta que están en la posición correcta.

Las herramientas de tensión son piezas planas y pequeñas que le permiten presionar la cerradura mientras utiliza la ganzúa.

Las ganzúas de rastrillo son parecidas a las ganzúas normales pero se emplean "rastrillando" dentro de la cerradura para alcanzar los pernos. Este movimiento rápido del rastrillo es el que resulta más eficaz para muchas personas, porque normalmente abre rápidamente la cerradura.

Para abrir una cerradura, siga estos pasos:

1. Inserte la herramienta de tensión en la bocallave y gírela en la misma dirección en la que se gira una llave. El secreto está en saber aplicar la presión correcta. Si aplica demasiada o demasiado poca, los pernos no se colocan en su sitio y la cerradura no gira. Al aplicar la cantidad exacta de presión se crea un pequeño saliente que desplaza el tambor lo suficiente para bloquear los huecos de los pernos.

2. Inserte la ganzúa y utilícela para levantar los pernos uno a uno hasta que sienta que encajan en su sitio. Escuchará un ligero chasquido cuando un perno superior entra en su sitio. Cuando todos los pernos estén posicionados, el tambor rotará libremente y la puerta se abrirá.

Ésta es una explicación muy simplificada de cómo abrir puertas con ganzúas. Si quiere más información al respecto, visite los siguientes sitios Web:

- `http://toool.us/`.
- `http://home.howstuffworks.com/home-improvement/household-safety/security/lock-picking.htm`.
- `http://www.lockpicking101.com/`.

Éstos son sólo algunos de los sitios Web dedicados al campo de la apertura de puertas con ganzúas. Es importante que practique abriendo puertas. Llevar un pequeño juego de herramientas puede ser la salvación cuando se encuentre ante un armario del servidor, un cajón o cualquier otro obstáculo cerrado con llave que contenga información jugosa.

Los juegos de ganzúas pueden ser tan pequeños como el que se muestra en la figura 7.2, que tiene el tamaño de una tarjeta de crédito.

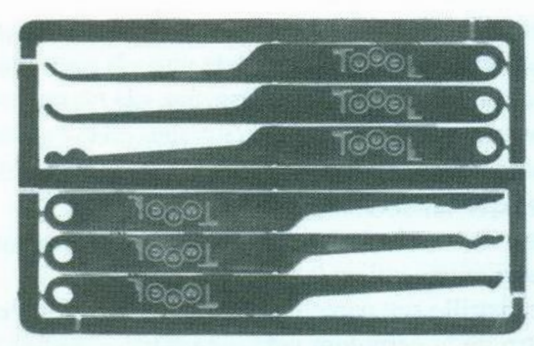


Figura 7.2. Este juego de ganzúas del tamaño de una tarjeta cabe perfectamente en una cartera o en un bolso.

También pueden ser un poco más voluminosos, como los que se muestran en las figuras 7.3 y 7.4.



Figura 7.3. Este juego es del tamaño de una navaja multiusos.

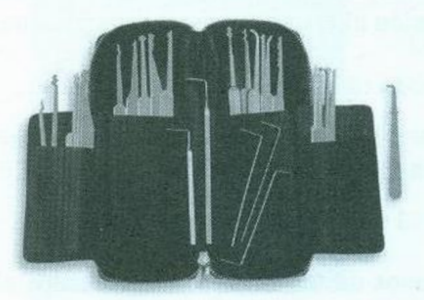


Figura 7.4. Este juego de ganzúas es más grande, pero contiene todo lo que puede necesitar.

Un buen consejo es que no permita que la primera vez que decida juguetear con una cerradura sea en una situación crítica. Lo que yo hice fue comprar varios candados de distintos tamaños. Cuando fui capaz de abrirlos todos compré un juego

de cerraduras para practicar, como las que se muestran en la figura 7.5. Estas cerraduras se fabrican con distinto número y tipo de pernos, pudiendo ir incrementando la dificultad. De esta manera, maximiza la efectividad de la sesión de práctica.

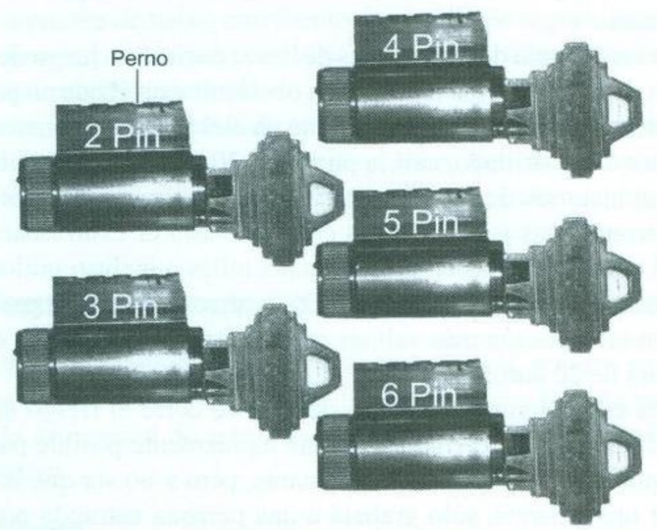


Figura 7.5. *Este tipo de cerraduras son transparentes para que puede ver qué tal lo está haciendo.*

A lo largo de mi vida profesional he acudido a algunas conferencias donde se preparaban montajes excelentes para practicar, como una pared de cerraduras casera. Por supuesto, cuando vaya recopilando información sobre su objetivo es buena idea que haga fotos o tome nota de los tipos, marcas y modelos de cerraduras con los que se puede encontrar. Esta información le ayudará a prepararse antes de entrar en acción.

Uso práctico

En las películas y la televisión la apertura de cerraduras con ganzúas se presenta como algo muy sencillo que se logra en cuestión de segundos una vez que se ha introducido la ganzúa. Por supuesto, habrá gente que lo haga así de bien, pero la mayoría de las personas necesitan tiempo, después de presionar demasiado incontables veces, frustrarse y aprender finalmente cómo rastrillar y abrir la cerradura. El rastrillado es un talento en sí mismo. Se emplea una ganzúa de rastrillo y lo mueve suavemente dentro y fuera de la cerradura aplicando una ligera presión a la herramienta de tensión. Esta técnica funciona con varios tipos de cerradura. Aprendiendo a rastrillar aprenderá a utilizar la herramienta de tensión correctamente y la sensación que se tiene cuando la cerradura se desbloquea.

Muchas empresas están empezando a utilizar el sistema RFID, tarjetas con placa magnética u otros tipos de sistemas electrónicos, que pueden llevarle a pensar que las ganzúas se están quedando obsoletas. Pero no es así. Aprender a abrir cerraduras con ganzúas es una habilidad que le será muy útil en sus auditorías de seguridad.

Aquí tiene un ejemplo de las ventajas de llevar encima un juego de ganzúas. En una actuación de seguridad me topé con un obstáculo con el que no podía emplear mis habilidades sociales: una puerta. Saqué un fiel juego de ganzúas de bolsillo y con la técnica del rastrillado, abrí la puerta en 30 segundos. Muchos ingenieros sociales tienen historias de este tipo, en las que saber un poco sobre cerraduras y tener las herramientas adecuadas les condujo hasta el éxito final. Muy a menudo se da el caso de que las empresas gastan miles o incluso millones de euros en equipamiento, cortafuegos, sistemas IDS y otros métodos de protección pero luego dejan su información más valiosa en un cuarto protegido por cristal barato y una cerradura de 20 euros.

La práctica es fundamental porque siempre se corre el riesgo de ser visto o descubierto. Debe abrir la cerradura lo más rápidamente posible para reducir el riesgo. En algunos lugares se instalan cámaras, pero a no ser que la cámara esté manejada por una persona, sólo grabará a una persona entrando por la fuerza y robando servidores.

Además, muchas cámaras pueden inutilizarse empleando sencillos métodos de luces LED dirigidas directamente a las lentes o llevando un gorro o una capucha para ocultar el rostro.

Abrir cerraduras magnéticas y electrónicas

Las cerraduras magnéticas son muy populares porque son baratas de mantener y proporcionan cierto nivel de seguridad al no tratarse de la cerradura clásica fácil de abrir con ganzúas. Hay cerraduras magnéticas de muchas formas, tamaños y solidez. No obstante, adolecen de cierta inseguridad: si se corta la corriente eléctrica la mayoría de cerraduras magnéticas se desconecta, desbloqueando la puerta. Esto sucede, por supuesto, si la cerradura no está conectada a una fuente de energía de seguridad.

El famoso ingeniero social y hacker Johnny Long, creador de Google Hacking Database y autor de *No Tech Hacking*, cuenta una historia sobre cómo eludió una cerradura de seguridad utilizando una percha y una toallita. Observando el movimiento de un empleado hacia la puerta se dio cuenta de que la cerradura estaba desconectada. También descubrió un espacio entre las puertas que era lo suficientemente grande para deslizar por él una toallita enganchada a una percha. Agitando la toallita pudo liberar la cerradura y entrar.

Recientemente, tuve la oportunidad de probar esta técnica. En efecto, con un poco de esfuerzo y probando diferentes longitudes con la percha, pude acceder en menos de dos minutos. Lo más asombroso para mí era que a pesar de la cantidad enorme de dinero gastado en las cerraduras profesionales y las puertas metálicas con cristales a prueba de balas, con fuente de energía de seguridad para las cerraduras y cerrojos de autobloqueo por si se corta la corriente, todo ese sistema se burlaba con una percha y un trapo.

Por supuesto, existen métodos de alta tecnología para abrir esas cerraduras. Se han creado clones de RFID, un pequeño dispositivo que puede capturar y replicar el código RFID desbloqueando las puertas. También existen máquinas para copiar llaves magnéticas.

Herramientas variadas para abrir cerraduras

Además de las herramientas de tensión y las ganzúas, pueden emplearse otras herramientas, como el cuchillo *shove*, la llave *bumping* y la cuña para candados. Dominando la utilización de estas herramientas podrá ganar acceso a cualquier lugar sin esfuerzo.

Cuchillo shove

El cuchillo *shove*, mostrado en la figura 7.6, está considerado como la forma más rápida de abrir puertas de oficina o cualquier puerta con pestillo en el pomo. Este cuchillo se puede deslizar en una posición en la que libera el pestillo sin dañar la puerta.

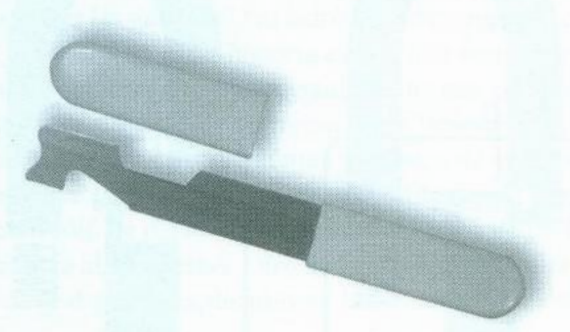


Figura 7.6. *Un típico cuchillo shove.*

Llaves bumping

Estas llaves llevan mucho tiempo utilizándose, pero han recibido mucha atención últimamente porque se han empleado en varios delitos. Las llaves *bumping* están diseñadas específicamente para introducirse en la cerradura y con un ligero

golpe alinear todos los pernos permitiendo que se pueda girar el tambor sin dañar la cerradura. La técnica básica consiste en introducir la llave y sacarla una o dos muescas; aplicar una ligera tensión en la llave y, utilizando el mango de un destornillador o un pequeño martillo, dar un golpe en la llave. Al hacerlo, se fuerzan los pernos hacia arriba permitiendo que el tambor gire. En la figura 7.7 puede ver una llave *bumping*.

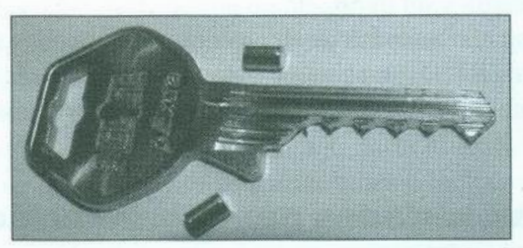


***Figura** 7.7. Una típica llave bumping.*

Cuñas para candados

Una cuña es una pequeña pieza de metal fino que se desliza dentro del candado y libera el mecanismo de bloqueo. La cuña se empuja a la base del hueco del cerrojo, separando el mecanismo de bloqueo y desbloqueando el candado. Puede ver el sistema en la figura 7.8.

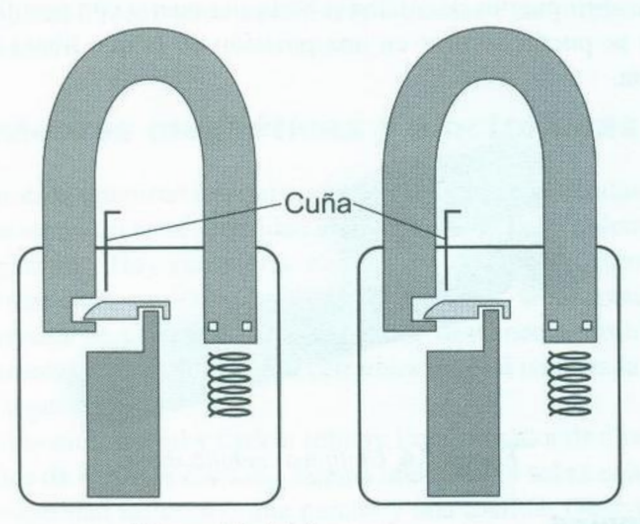


***Figura** 7.8. Así funciona una cuña.*

La figura 7.9 muestra cuñas profesionales pero también puede fabricar una casera utilizando una lata de aluminio.

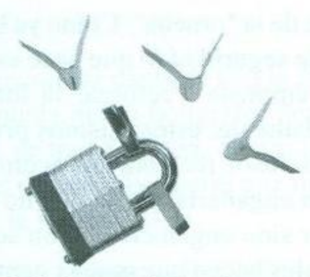


Figura 7.9. *Cuñas profesionales para candados.*

Puede encontrar historias sobre lo sencillo que resulta abrir puertas con cadenas y candados. Este vídeo (`www.youtube.com/watch?v=7INIRLe7x0Y`) muestra al atacante atar una banda de goma en la cadena de una puerta de hotel. Después, la tensión natural de la banda consigue liberar la cadena. Por su parte, el Massachusetts Institute of Technology (MIT) distribuye de manera gratuita una guía sobre apertura de puertas (`www.lysator.liu.se/mit-guide/MITLockGuide.pdf`) mucho más profunda que la breve introducción incluida en ese capítulo.

Puede que se esté preguntando si existen cerraduras imposibles o muy difíciles de abrir. La cerradura Bump Proof BiLock es una de ésas (`www.wholesalelocks.com/bump-proof-bilock-ult-360.html`). Sus dos cilindros hacen que sea prácticamente imposible de abrir con ganzúas. Uno de los problemas más comunes que he detectado en mi carrera no es tanto la elección de la cerradura sino la seguridad que rodea a la cerradura. A menudo, una empresa compra una cerradura de gran resistencia que requiere de biometría y claves de acceso para entrar en el cuarto de servidores pero, luego, al lado de la puerta, hay una ventana con un cristal sencillo. ¿Para qué usar las ganzúas? Un ladrón puede romper el cristal y entrar sin mucho esfuerzo. La moraleja de la historia es que una cerradura por sí sola no le mantiene seguro. La seguridad es una mentalidad no una pieza de ferretería.

No es necesario ser un experto cerrajero, pero poseer ciertos conocimientos básicos sobre cómo funcionan las cerraduras y un poco de experiencia abriéndolas con ganzúas puede marcar la diferencia en sus auditorías de seguridad.

Esta explicación sólo ha rozado la superficie del tema de las herramientas que se pueden utilizar para abrir puertas. Otro de los equipos de valor incalculable son los dispositivos de grabación, explicados en la siguiente sección.

Cámaras y dispositivos de grabación

El tema de las cámaras y los dispositivos de grabación puede sonar tan "voyerista" que muchas veces surge la pregunta: "¿Por qué? ¿Por qué emplear cámaras y dispositivos de grabación ocultos en una auditoría?". Buena pregunta. Y tiene una respuesta en dos partes: por protección y para reunir pruebas.

Expliquemos el concepto de la "prueba". Como ya hemos mencionado, cuando lleva a cabo una auditoría de seguridad lo que hace es poner a prueba a la gente. Consiste en ayudar a una empresa a reforzar la infraestructura humana para ser más segura. Desgraciadamente, estos mismos principios se aplican cuando los ingenieros sociales maliciosos realizan sus acciones. Muchas personas son reacias a pensar que pueden engañarlas hasta que no ven cómo han engañado a otro. La vergüenza de haber sido engañado con un sencillo ataque o el miedo a ciertas repercusiones laborales hacen que mucha gente prefiera pretender que el ataque nunca ha sucedido. Un dispositivo de grabación proporciona esa prueba, además de servir para enseñar al auditor y al cliente las cosas a las que deben prestar atención.

Nunca debe utilizar estos dispositivos con la intención de poner en problemas o en evidencia a un empleado. No obstante, la información que obtiene a través de estos aparatos proporciona una estupenda herramienta de aprendizaje para mostrar cómo y por qué alguien de la plantilla ha caído en la trampa de un pretexto de ingeniería social. La prueba de un ataque exitoso ayuda a educar a la empresa y a su personal sobre cómo deben reaccionar en estas situaciones. En otras palabras, cómo detectar estos ataques para evitarlos o mitigarlos.

La segunda razón para emplear sistemas de grabación es por protección, principalmente en el caso de los auditores profesionales. ¿Por qué? Es imposible detectar todas las microexpresiones, gestos faciales y pequeños detalles que le pueden ser útiles. Capturar esta información le da material para analizar en busca de todos los detalles que necesita para el ataque. También proporciona protección porque puede probar lo que ocurrió y lo que no ocurrió, pero sobre todo, permite que no tenga que depender de la memoria. Además, es una buena forma de estudiar los intentos exitosos y fallidos para seguir mejorando como ingeniero social.

Este principio lo emplean las fuerzas del orden. La policía graba las situaciones en las que paran un vehículo en la carretera, las entrevistas y los interrogatorios, por protección, formación y como prueba para utilizarse en un juicio.

Estos principios también se aplican en el caso de la grabación de audio. Registrar una llamada de teléfono o una conversación en un aparato de grabación sirve los mismos propósitos que los mencionados para el caso del vídeo. Es importante señalar que en muchos lugares del mundo es ilegal grabar a alguien sin su consentimiento. Asegúrese de que en el contrato que firma con la empresa se especifica la opción de emplear dispositivos de grabación.

Los aparatos de grabación se fabrican de todas las formas y tamaños. Yo tengo un grabador de voz que es un bolígrafo. Puedo colocarlo en el bolsillo de la camisa y graba con precisión hasta a 6 metros de distancia. Tiene una capacidad de almacenamiento de 2 GB, por lo que puedo grabar hasta dos horas de conversación.

Cámaras

Hoy en día se pueden encontrar cámaras con la forma de un botón; de un bolígrafo; escondidas en la punta de un bolígrafo; dentro de un reloj, de un osito de peluche, en una cabeza de tornillo falsa, dentro de una alarma antiincendios; resumiendo, prácticamente en cualquier parte que imagine. No es difícil colocar una cámara como muestra la figura 7.10.

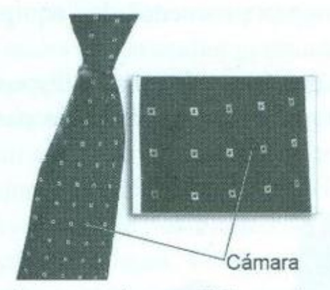


Figura 7.10. *La cámara está escondida en el nudo de la corbata.*

Sí, aunque no lo crea, esa corbata esconde una cámara a todo color que funciona con una batería de 12 voltios y que se conecta a un pequeño dispositivo de grabación. Lo capta todo en un ángulo de 70 grados.

Emplear un dispositivo como éste le da mucha ventaja. Puede concentrarse en su pretexto o en su labor de recopilación de información sin tener que preocuparse de recordar cada detalle más tarde.

Me gusta contar una historia de una ocasión en la que utilicé un sistema de grabación de audio en una auditoría que realizaba a un parque temático que vendía billetes *on-line*. En el parque había una taquillera en una ventanilla que utilizaba un sistema operativo Windows. El pretexto era que había comprado los billetes *on-line* pero había olvidado imprimirlos. Los había guardado en formato PDF y me los había enviado a mí mismo por correo electrónico. Dije algo como esto: "Ya sé que le estoy pidiendo algo un poco extraño, pero mi hija vio su anuncio en un restaurante. Volvimos al hotel y compramos los billetes *on-line* con el código de descuento y después nos dimos cuenta de que no podíamos imprimirlos. Los he guardado en PDF en mi cuenta de correo. ¿Puedo conectarme un momento a mi correo electrónico o pedirle que se conecte usted para conseguir el documento?". Por supuesto, los "niños" me estaban esperando y como padre no quería defraudarlos. En efecto, en cuanto la empleada hico clic en el documento, no aparecieron los billetes, sino que se activó un código malicioso que estaba programado para darme acceso a su ordenador y empezar a recopilar información. Grabar la conversación, el método empleado y las fibras sensibles que se tocaron sirvió para formar a esta empresa para que este ataque no se repita a un coste de miles de euros.

Existe un dispositivo que emplea una tarjeta de teléfono móvil de prepago para enviar archivos de audio a través de una señal telefónica al número que se programe. O también se puede llamar al teléfono móvil y escuchar en directo lo que está teniendo lugar. Este aparato puede ahorrar muchas horas de trabajo obteniendo contraseñas o información personal.

Podríamos pasar horas y dedicar docenas de páginas a hablar sobre las ingeniosas cámaras que existen en el mercado. Las figuras 7.11 y 7.12 le muestran algunos modelos de un famoso proveedor de "equipamiento de espía" (`www.spyassociates.com`).

Todas las imágenes son de cámaras ocultas o dispositivos de audio, aunque no lo crea. Puede utilizar cualquiera de estos aparatos para grabar disimuladamente al objetivo para su posterior análisis.



***Figura 7.11.** Todos estos aparatos capturan imagen en color y sonido a través de una cámara excepto el bolígrafo, que sólo graba audio.*



***Figura 7.12.** Estos dispositivos también capturan imagen y sonido a través de cámaras ocultas.*

Emplear las herramientas de un ingeniero social

La sección anterior señala algunos de los tipos de aparatos de grabación existentes, pero es necesario saber también cómo utilizarlos. Aunque parezca increíble, la utilización de cámaras y otros dispositivos de grabación sigue los mismos principios que cualquier otra herramienta de la ingeniería social, como el pretexto o las maniobras de recopilación de información.

Practicar es fundamental. Si no elige bien el lugar donde va a esconder una cámara o un dispositivo de audio puede acabar grabando imágenes del techo o una voz apagada. Es necesario preparar el equipo que va a llevar y encontrar el lugar adecuado para colocar la cámara o el dispositivo de audio. Pruebe a sentarse o andar para ver cómo afectan estos movimientos a la calidad de la grabación.

Para los auditores de seguridad profesionales debo insistir en la importancia de establecer claramente en el contrato la posibilidad de grabar. Hacerlo sin permiso puede convertirse en una pesadilla legal. Compruebe las leyes territoriales para confirmar que no hay ningún problema por emplear estos aparatos.

Un ingeniero social bajo ningún concepto debe grabar a gente en situaciones comprometidas o íntimas.

El tratamiento de este tema puede alargarse mucho más, pero espero que este breve acercamiento a estas herramientas y a cómo emplearlas pueda ampliar sus opciones como ingeniero social. En la siguiente sección, doy algunos ejemplos de la utilización de algunas herramientas muy útiles.

Utilización del rastreador GPS

En ocasiones, es necesario seguir la pista al objetivo antes o después de que se vayan de la oficina. Las paradas que hace antes de llegar al trabajo pueden darle mucha información sobre él. Recopilar y analizar esta información puede ayudarle a desarrollar el pretexto adecuado o a preparar unas buenas preguntas para sonsacarle las respuestas apropiadas. Conocer sus horarios de inicio y fin de la jornada también puede ser útil para lanzar un ataque del *red team* (equipo rojo), cuya meta es entrar en la empresa objetivo y recuperar activos valiosos para demostrar a la empresa sus debilidades. Se puede rastrear a la gente de muchas maneras; una de ellas es emplear un dispositivo diseñado para tal efecto, como el rastreador GPS; por ejemplo el eficiente SpyHawk SuperTrak GPS Worldwide Super TrackStick USB Data Logger disponible en `www.spyassociates.com`. El precio de estos aparatos oscila entre los 200 y los 600 euros. El SpyHawk SuperTrak se adhiere magnéticamente a un vehículo y puede almacenar grandes cantidades de datos sobre el objetivo. La siguiente sección ofrece un recorrido desde la preparación a la utilización de este pequeño dispositivo.

El SpyHawk SuperTrak GPS TrackStick

El software necesario para utilizar este aparato se instala de manera muy sencilla, simplemente ejecutando el software que viene con el aparato y siguiendo los pasos que se muestran en pantalla instalará el software necesario. Se instala sin problemas y el programa también es sencillo. La pantalla de TrackStick, mostrada en la figura 7.13, es muy intuitiva y fácil de manejar.

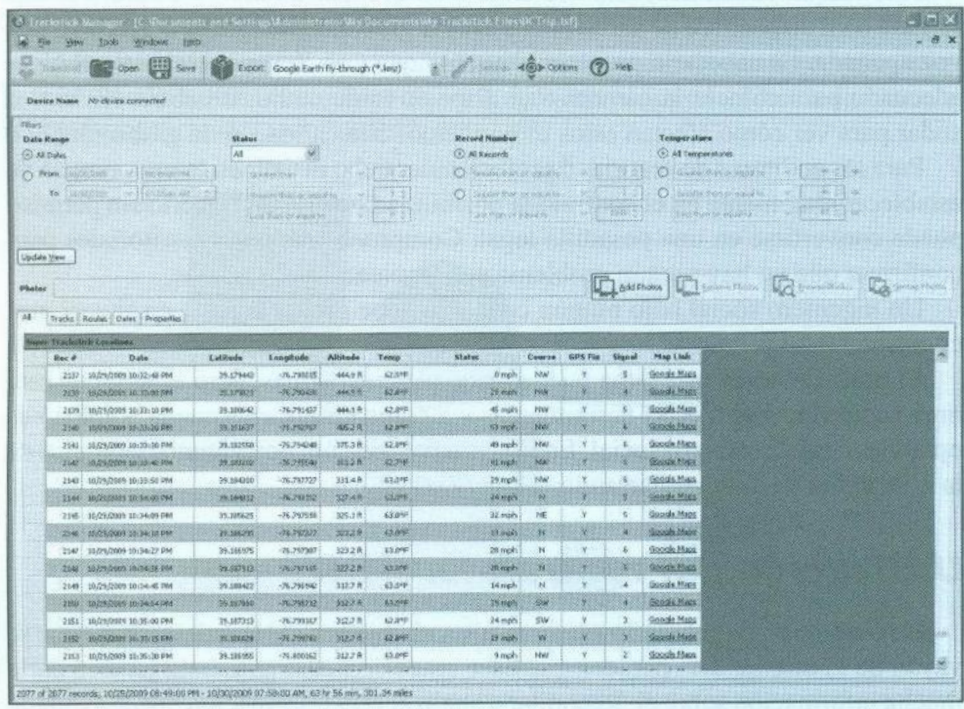


Figura 7.13. *El TrackStick Manager emplea una interfaz muy sencilla y fácil de utilizar.*

Como puede ver, ofrece opciones para elegir registros horarios, zonas horarias y muchas otras opciones a medida.

Utilizar el SpyHawk TrackStick

El SpyHawk SuperTrak GPS Worldwide Super TrackStick es un aparato muy ligero y fácil de manejar y esconder. Tiene un interruptor de encendido/apagado y utiliza tecnología avanzada. Cuando detecta movimiento se enciende y empieza a registrar datos. Cuando el movimiento se detiene por un tiempo determinado, detiene el registro.

Las instrucciones explican que el aparato se debe esconder en algún lugar con los imanes contra el metal y con el aparato boca arriba y dirigido hacia una zona de plástico. Siempre existe la preocupación de perder el dispositivo en su primer intento, por lo que encontrar un lugar seguro bajo el capó evita preocupaciones y proporciona un buen acceso para la vista aérea. Una vez que tenga acceso (ya sea al interior o al exterior) al coche del objetivo, encuentre un lugar seguro, en el interior del guardabarros, en la parte trasera del coche o en el maletero. Cualquier sitio donde haya metal servirá. Si puede acceder al interior, abra el capó y colóquelo en algún lugar en el compartimento del motor, de esta forma no tendrá que preocuparse de que se pierda o lo puedan descubrir. En mis primeras pruebas, encontré un lugar en el motor para colocar el dispositivo. Incluso a través del metal del capó funcionó perfectamente. Otra idea es colocarlo en el maletero bajo la alfombrilla o sobre las luces traseras. A nivel personal, cuando realicé esta prueba, el aparato se mantuvo cinco días recopilando datos, algunos de los cuales puede ver en las siguientes figuras. Como muestra la figura 7.14, parece que al objetivo le gusta correr.

All | Tracks | Routes | Dates | Properties

Super Trackstick Locations

Rec #	Date	Latitude	Longitude	Altitude	Temp	Status	Course	GPS Fix	Signal	Map Link
212	10/25/2009 09:55:16 PM	40.944602	-76.021046	1588.4 ft	67.7°F	84 mph	S	Y	3	Google Maps
213	[illegible]	40.942953	-76.024602	[illegible]	67.7°F	[illegible]	S	Y	2	Google Maps
214	10/25/2009 09:59:36 PM	40.940080	-76.023738	1593.2 ft	67.4°F	88 mph	S	Y	4	Google Maps
215	[illegible]	[illegible]	-76.022563	[illegible]	67.6°F	[illegible]	S	Y	4	Google Maps
216	10/25/2009 09:59:54 PM	40.934292	-76.019250	1675.5 ft	67.4°F	85 mph	SE	Y	3	Google Maps
217	[illegible]	[illegible]	[illegible]	[illegible]	67.4°F	88 mph	SE	Y	[illegible]	Google Maps
218	10/25/2009 10:00:08 PM	40.931225	-76.015792	1686.0 ft	67.4°F	81 mph	SE	Y	3	Google Maps
219	10/25/2009 10:00:16 PM	40.929418	-76.013752	1686.0 ft	67.6°F	80 mph	SE	Y	2	Google Maps
220	10/25/2009 10:00:24 PM	40.927317	-76.012177	1686.0 ft	67.4°F	85 mph	S	Y	3	Google Maps
221	10/25/2009 10:00:32 PM	40.924518	[illegible]	1686.0 ft	67.6°F	86 mph	S	Y	2	Google Maps
222	10/25/2009 10:00:40 PM	40.922535	-76.012137	1686.0 ft	67.4°F	83 mph	S	Y	3	Google Maps
223	10/25/2009 10:00:48 PM	[illegible]	-76.013100	1686.0 ft	67.6°F	79 mph	SW	Y	2	Google Maps
224	10/25/2009 10:00:56 PM	40.916130	-76.016463	1686.0 ft	67.3°F	87 mph	SW	Y	3	Google Maps
225	10/25/2009 10:01:02 PM	40.914030	-76.018277	1686.0 ft	67.3°F	88 mph	SW	Y	3	Google Maps
226	10/25/2009 10:01:05 PM	40.912747	-76.020038	1686.0 ft	67.4°F	87 mph	SW	Y	3	Google Maps
227	10/25/2009 10:01:10 PM	[illegible]	-76.021702	1686.0 ft	67.4°F	83 mph	SW	N	3	Google Maps
228	10/25/2009 10:01:27 PM	40.908272	-76.023632	1686.0 ft	67.2°F	81 mph	SW	Y	3	Google Maps

Figura 7.14. *Al objetivo le gusta correr.*

Marcas de hora, fecha y duración le ayudan a registrar el movimiento del objetivo, como muestra la figura 7.15.

All | Tracks | Routes | Dates | Properties

Super Trackstick Dates

Date	Time Period	Record #'s	Total Duration	Distance
[illegible]	08:49:00 PM - 12:00:54 AM	2 - 919	3 hr 11 min	175.59 mi
10/26/2009	12:00:00 AM - 12:00:40 AM	920 - 1373	13 hr 54 min	61.42 mi
10/27/2009	12:00:40 AM - 12:00:00 AM	1373 - 1610	15 hr 13 min	13.02 mi
10/28/2009	12:00:00 AM - 12:00:00 AM	1610 - 1908	14 hr 35 min	16.85 mi
10/29/2009	12:00:00 AM - 10:54:45 PM	1908 - 2244	14 hr 24 min	27.79 mi
10/30/2009	05:19:00 AM - 07:58:00 AM	2245 - 2349	2 hr 39 min	6.51 mi

Figura 7.15. *Rastreando los movimientos del objetivo.*

La figura 7.16 muestra los iconos en un mapa de Google Earth. Indican velocidad, hora, tiempo parado y mucho más.

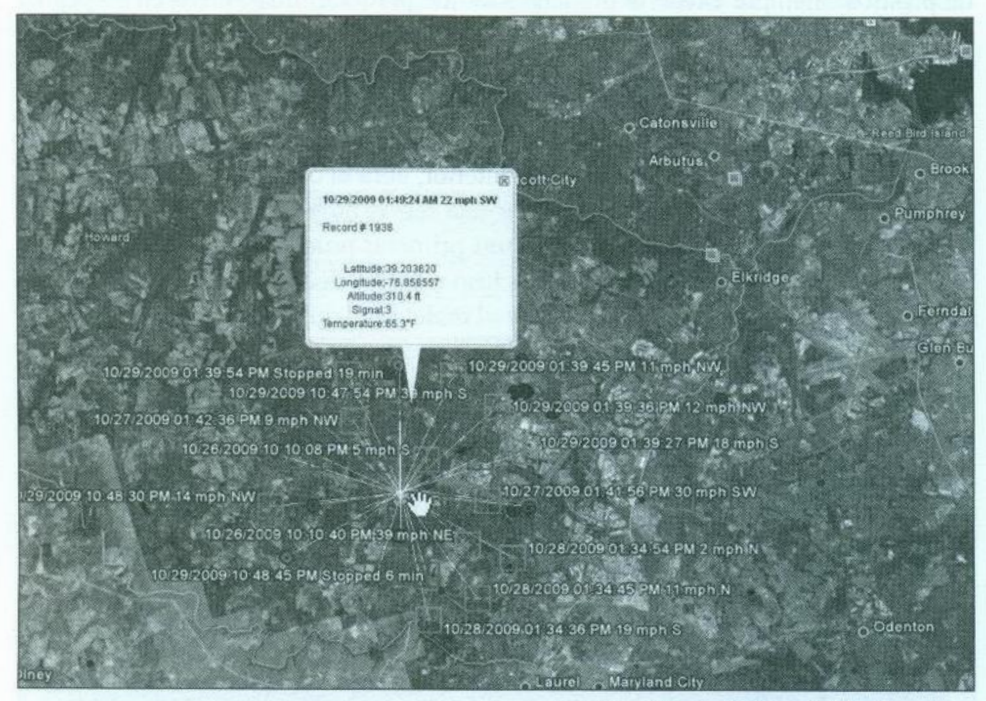


__Figura 7.16.__ Representación de los datos del dispositivo en Google Earth.

Como puede ver en la figura 7.17, el software crea buenos mapas de la ruta completa.

Utilizando Google Earth o Google Maps puede incluso obtener primeros planos (véase la figura 7.18).

Revisar los datos del rastreador GPS

En la recopilación de datos es donde encontrará mayores ventajas. Al ser capaz de registrar cada vez que el director de la empresa para a tomar un café, cuál es su tienda favorita y en qué gimnasio entrena, podrá planificar su ataque con una probabilidad de éxito muy alta.

Conocer las localizaciones y las paradas le permite saber dónde y cuándo puede ser un buen momento para clonar una placa RFID o para hacer una copia de una llave. Y la gran ventaja es que podrá hacer todo esto sin tener que acosar al objetivo. Las siguientes figuras muestran cómo estos detalles pueden poner al atacante en situación ventajosa.

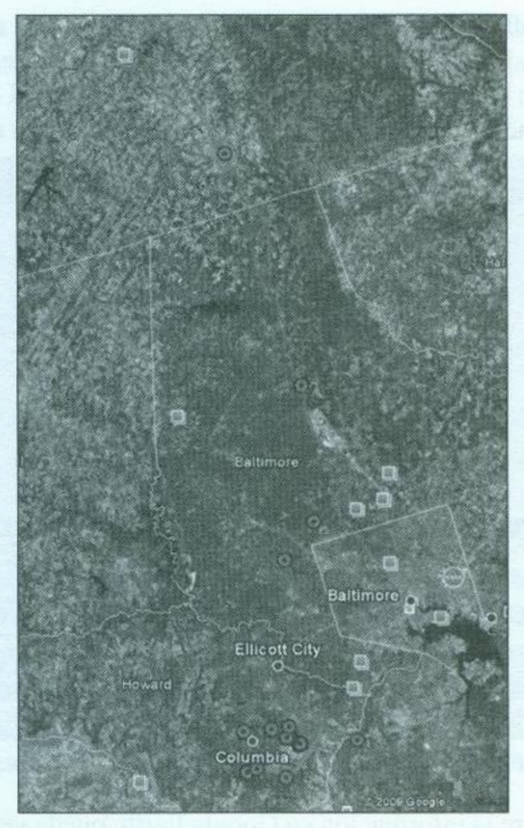


Figura 7.17. *Trazando el mapa de la ruta del objetivo con SuperTrack.*

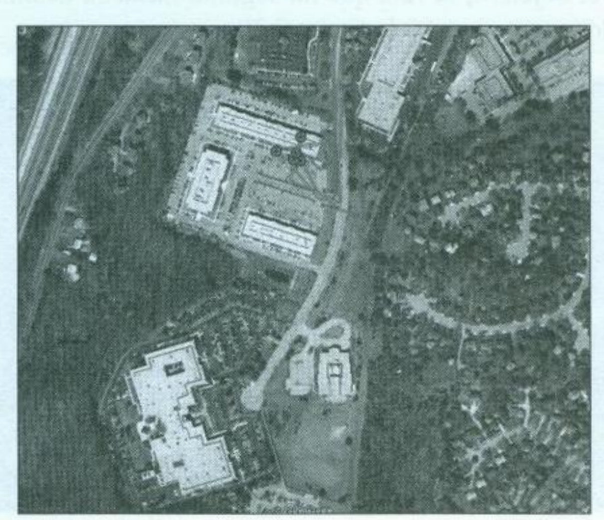


Figura 7.18. *Podemos seguir en detalle los viajes del objetivo.*

Observe el detalle de la figura 7.19. Puede ver la velocidad a la que conduce el objetivo y la fecha y la hora de sus paradas. Si quiere ver la localización en más detalle, puede hacer clic en el vínculo de Google Earth. Haga clic en el botón **Export** para exportar la información a un mapa interactivo de Google Earth o Google Maps.

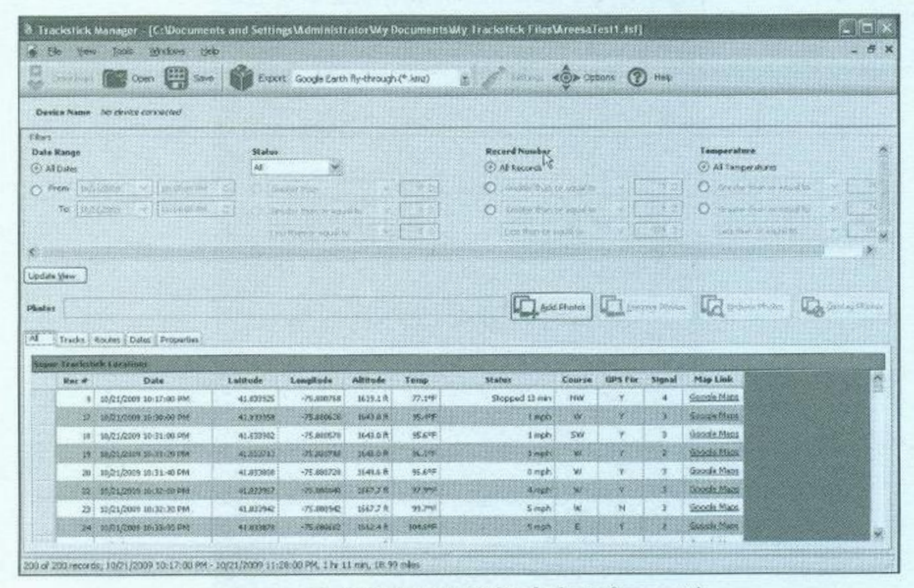


Figura 7.19. La presentación de la información.

Una vez que abre la información en Google Earth, puede ver los puntos donde se ha detenido el objetivo, la ruta que ha seguido hasta su destino y los lugares donde ha parado, como muestra la figura 7.20.

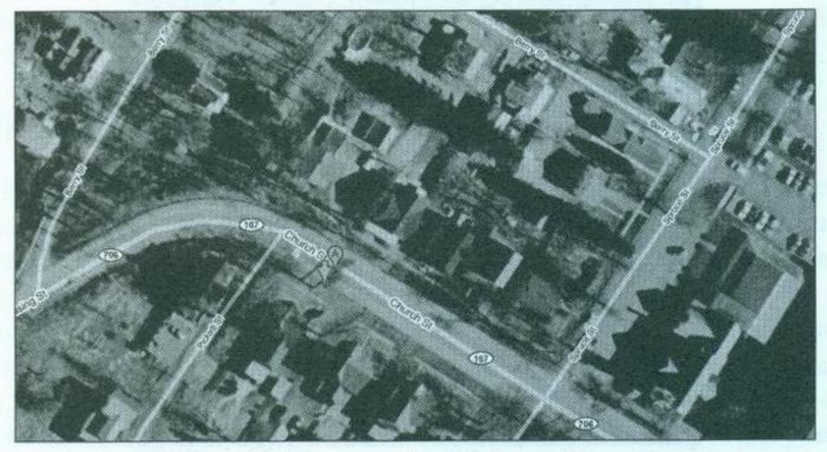


Figura 7.20. Las paradas a lo largo del camino.

Si quiere ver su ruta completa, no hay problema. Simplemente exporte la ruta a uno de los muchos formatos disponibles, tal y como se puede observar en la figura 7.21.

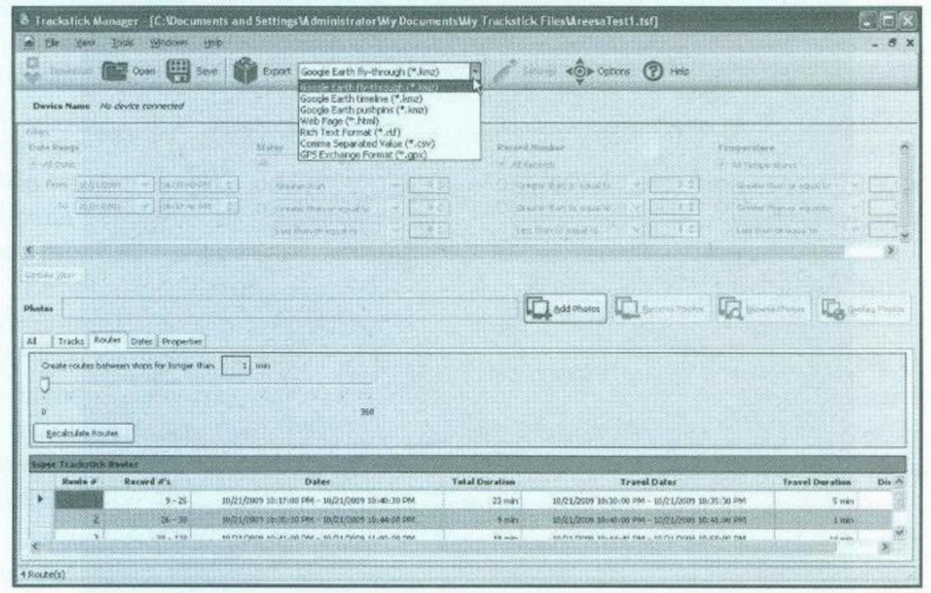


Figura 7.21. *Exportando la ruta completa del objetivo.*

La figura 7.22 muestra la información exportada y visualizada en Google Maps.

Esta breve sección no puede abordar todas las herramientas disponibles para el ingeniero social. Las claves para lograr el éxito son la práctica y la investigación. Conocer las herramientas de las que dispone puede marcar la diferencia en sus auditorías.

No obstante, eso es sólo la mitad de la batalla, porque después debe practicar, practicar y practicar. Es fundamental aprender a utilizar las herramientas adecuadamente.

En el ámbito conceptual de la ingeniería social localizado en `www.social-engineer.org`, reviso muchas herramientas que puede emplear para mejorar su rendimiento.

Las herramientas físicas son sólo una pequeña parte necesaria para tener éxito. Todas las herramientas físicas están respaldadas por una garantía de calidad y una concienzuda recopilación de información, como se explica en el capítulo 2. La siguiente sección aborda algunas de las herramientas de recopilación de información más asombrosas del mundo.



Figura 7.22. La ruta del objetivo presentada en Google Maps.

Herramientas de recopilación de información on-line

Como hemos explicado en este libro, la recopilación de información es un aspecto clave de la ingeniería social. No dedicar el tiempo necesario a este punto conducirá al fracaso de la acción de seguridad. Hoy en día, hay muchas herramientas disponibles para recolectar, catalogar y utilizar los datos recopilados.

Esas herramientas pueden cambiar literalmente el modo en que un ingeniero social ve y utiliza la información. Los auditores de seguridad ya no tienen que limitarse a búsquedas rutinarias; esas herramientas desvelan para ellos todas las fuentes disponibles en Internet.

Maltego

Reunir y catalogar la información suele ser un punto débil para mucha gente. ¿Qué sucedería si existiera una herramienta que permitiera realizar docenas de búsquedas específicas de un dominio, dirección IP o incluso una persona? ¿Qué sucedería si le diera la ponderación de sus búsquedas, diferenciando la que parece más importante de la que no? ¿Qué le parecería si esta herramienta tuviera una interfaz gráfica de usuario (GUI, *Graphical User Interface*) que mostrara todo en objetos con codificación cromática que puede exportar y utilizar? Y, por encima de todo, ¿qué le parecería si hubiera disponible una versión gratuita de este producto?

Le presento Maltego. Maltego es la herramienta soñada del ingeniero social. Los creadores de este increíble producto son los chicos de Paterva (`www.paterva.com`). Maltego tiene una versión para descarga gratuita desde su sitio Web, que se incluye también en todas las ediciones del BackTrack4. Si quiere eliminar las limitaciones de la edición gratuita (como el número de transformaciones que puede ejecutar y grabar datos), por unos 600 euros puede conseguir la versión completa.

La mejor manera de explicar el poder de Maltego es contar una historia sobre una auditoría en la que trabajé. Me encargaron la tarea de auditar a una pequeña empresa que tenía muy poca presencia en la Web. El objetivo era alcanzar al director general pero estaba obsesivamente protegido y apenas utilizaba Internet. Como dueño de una imprenta, estaba dedicado en cuerpo y alma a su negocio y no utilizaba al máximo los avances tecnológicos. Parecía que ésta iba a ser una tarea complicada.

Recurrí a Maltego. Utilizando el dominio de la empresa y vinculando todas las direcciones de correo electrónico con información de Whois y del propio dominio, conseguí una buena base con la que empezar a buscar. Profundicé un poco más averiguando si la dirección de correo del director se estaba empleando en algún otro sitio Web u otra URL. Descubrí que había escrito un par de reseñas para un restaurante de otro estado.

Al leer la reseña era totalmente evidente que había visitado el restaurante cuando había ido a ese estado para visitar a la familia. Incluso nombraba a su hermano en la reseña.

Con unas cuantas búsquedas más en Maltego localicé a sus padres y a su hermano en esa zona. Utilicé el apellido para hacer más búsquedas y encontré algunos vínculos que mencionaban la utilización de otra dirección de correo electrónico de un negocio que tuvo en aquel lugar para discutir un problema que tuvo con la parroquia local y su cambio a una distinta. Más tarde, descubrí una entrada de un

blog que vinculaba su página de Facebook con fotografías de su familia al salir de un partido de béisbol de su equipo favorito. Esto es lo que pude encontrar en menos de dos horas utilizando Maltego:

- Su comida favorita.
- Su restaurante favorito.
- El nombre y la edad de sus hijos.
- Que estaba divorciado.
- El nombre de sus padres.
- El nombre de su hermano.
- Donde creció.
- Su religión.
- Su equipo favorito.
- El aspecto de toda su familia.
- Su antiguo negocio.

Un día más tarde envíe un paquete al objetivo con información sobre una rifa para negocios locales. La oferta era que si ganaba conseguía una cena gratis en el restaurante que me constaba como su preferido y tres billetes de regalo para ir a ver a su equipo de béisbol favorito. Todo lo que se le pedía a la empresa para participar era que aceptara mantener una reunión con el representante de ventas para hablar una obra de caridad local. Si la empresa accedía a esa reunión su nombre entraría a formar parte de la rifa y tendría la opción de conseguir los billetes para el partido. El nombre de mi pretexto era "Joe". Preparé el argumento para una llamada al director. Mi meta era que aceptara un PDF en el que se explicaba todo el asunto. Cuando hiciera la llamada ya habría recibido el paquete, así que podría emplear el argumento: "Sí, está esperando mi llamada".

Mientras estaba al teléfono con "Joe", el director aceptó y abrió un correo electrónico con todos los detalles de la rifa y con un archivo con código malicioso, que me permitiría obtener acceso a su red.

Por supuesto, no aparecía nada en su pantalla y se frustraba al comprobar que Adobe se bloqueaba constantemente. Le dije: "Siento que no pueda abrir el archivo; incluiremos su nombre en la rifa y le enviaremos información adicional esta misma tarde". Pero, antes de enviar este nuevo paquete, convoqué una reunión para explicar cómo se había puesto en una situación comprometida el objetivo.

La gran mayoría del éxito de esta acción se debía a la utilización de una herramienta: Maltego. Me ayudó a recopilar, organizar y catalogar los datos para hacer buen uso de ellos. ¿Cómo me ayudó Maltego en esta acción?

Piense en Maltego como una base de datos relacional que encuentra vínculos en Internet entre "pedazos" de información (llamados "entidades", en la aplicación). Maltego también evita gran parte del trabajo duro de la extracción de datos como las direcciones de correo electrónico, sitios Web, direcciones IP e información de dominios. Por ejemplo, puede buscar cualquier dirección de correo dentro del dominio del objetivo de manera automática en pocos pasos. Simplemente añadiendo la transformación de "EMAIL" (correo electrónico) en la pantalla y haciendo clic en el cuadro y escribiendo el correo electrónico que quiere buscar, consigue un resultado como el que se puede ver en la figura 7.23.

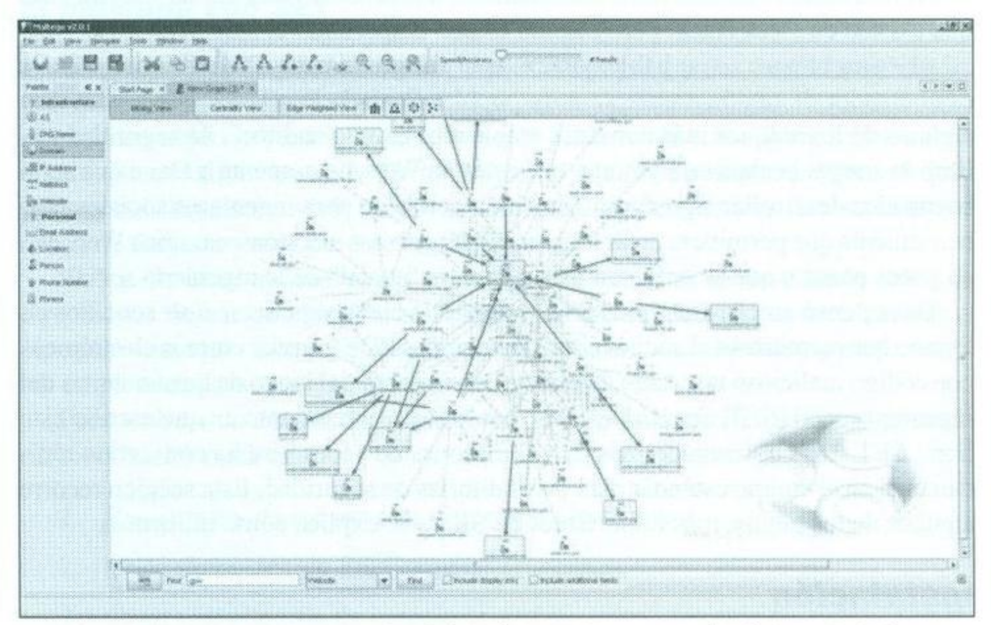


Figura 7.23. *Una representación de la información que puede obtener de Maltego.*

¿Por qué utilizar Maltego?

Maltego automatiza gran parte del proceso de recopilación de información y correlación de datos a gran escala para el usuario, ahorrando horas de búsquedas de información en Google y de determinar cómo se relaciona esa información. El verdadero poder de Maltego reside en esa capacidad para relacionar los datos. Aunque la extracción de datos es útil, descubrir las relaciones entre la información es lo que verdaderamente ayuda al auditor de seguridad.

En `www.social-engineer.org/se-resources/` he subido algunos vídeos que explican cómo utilizar Maltego para sacarle el máximo partido. En la historia anterior, Maltego jugó un papel muy importante para el éxito del ataque, pero la situación comprometida se consiguió con otra herramienta asombrosa.

SET: El juego de herramientas del ingeniero social

Los ingenieros sociales emplean mucho tiempo en perfeccionar el aspecto humano de sus habilidades; sin embargo, muchos vectores de ataque requieren la habilidad de crear correos electrónicos o documentos PDF codificados con código malicioso.

Ambas cosas se pueden hacer manualmente utilizando algunas de las herramientas que existen en BackTrack, pero cuando estaba empezando el sitio Web `www.social-engineer.org` hablé con un buen amigo llamado Dave Kennedy. Dave es el creador de una herramienta muy popular llamada FastTrack que automatiza algunos de los ataques más comunes empleados en una auditoría de seguridad utilizando *scripts* hechos en Python y una interfaz Web. Le comenté a Dave que sería buena idea desarrollar algo como FastTrack pero sólo para ingenieros sociales; una herramienta que permitiera crear archivos PDF, correos electrónicos, sitios Web, etc. en pocos pasos y que se enfocara más a la parte "social" de la ingeniería social.

Dave pensó en el asunto y decidió que podría crear algunos *scripts* sencillos en Python que permitieran al auditor crear documentos PDF y enviar correos electrónicos con código malicioso insertado. Ése fue el nacimiento del juego de herramientas del ingeniero social (SET, *Social Engineer Toolkit*). En el momento en que escribo este libro, SET se ha descargado más de 1,5 millones de veces y se ha convertido rápidamente en el equipo estándar para las auditorías de seguridad. Esta sección recorre algunos de los puntos más importantes de SET y le explica cómo utilizarlos.

Instalación

La instalación es simple. Sólo necesita tener instalado Python y el Metasploit Framework. Ambos están incluidos en la distribución BackTrack, por lo que no hay que preocuparse por su instalación. En BackTrack incluso SET ya está instalado. En caso de que no lo esté o si está empezando desde cero, la instalación es simple. Navegue al directorio que desea incluir y ejecute este comando en una consola de comandos:

```
svn co http://svn.secmaniac.com/social_engineering_toolkit set/
```

Después de ejecutar este comando, tendrá un directorio llamado `set` que contiene todas las herramientas de SET.

Ejecutar SET

El proceso de ejecutar SET también es sencillo. Escribiendo `./set` en el directorio `set` se inicia el menú principal.

Esto le muestra exactamente el aspecto del menú SET. En www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Social_Engineer_Toolkit_%28SET%29, encontrará un tutorial exhaustivo y profundo explicando cada opción del menú, pero las siguientes secciones abordan dos de los aspectos más utilizados de SET.

Primero, se explica el ataque denominado *phishing* y, a continuación, abordamos la clonación de sitios Web.

El phishing con SET

El término *phishing* hace relación al proceso por el que los estafadores "lanzan una gran red" (*fishing* en inglés significa pescar) sobre las direcciones de correo electrónico objetivo para intentar atraer a la gente hacia sitios Web, hacerle abrir documentos maliciosos o revelar información que puede emplearse para ataques posteriores. Para sobrevivir en el mundo actual de Internet, es fundamental ser capaz de detectar y mitigar estos ataques.

SET permite al auditor poner a prueba a sus clientes desarrollando listas de direcciones de correo electrónico objetivo y registrando cuántos empleados cayeron en el ataque. Esta información puede utilizarse más adelante para formar a los empleados para detectar y evitar estas trampas.

Para realizar un ataque de *phishing* en SET, elija la opción 1. El programa le ofrecerá varias opciones:

1. Realizar un ataque masivo vía correo electrónico.
2. Crear datos de tipo FileFormat.
3. Crear una plantilla de ingeniería social.

Eligiendo la primera opción se lanza el ataque de *phishing* a direcciones de correo electrónico. Con la segunda opción se crea un documento PDF malicioso u otro tipo de archivo para enviar a través del correo electrónico. La tercera opción se selecciona para crear plantillas para su uso posterior.

Lanzar un ataque desde SET es tan sencillo como elegir la opción adecuada en el menú y hacer clic en **Launch** (Lanzar). Por ejemplo, si quiero lanzar un ataque para enviar por correo electrónico al objetivo un PDF malicioso disfrazado de informe técnico, elegiré la opción 1, Realizar un ataque masivo vía correo electrónico.

Después elegiré un vector de ataque (opción 6) que estaba presente en muchas versiones del Adobe Acrobat Reader: `Adobe util.printf() Buffer Overflow`.

Las siguientes opciones se emplean para preparar la parte técnica del ataque. Emplee Metasploit para conseguir una consola inversa o una conexión inversa desde el ordenador del objetivo y el puerto de comunicación utilizado para evitar el IDS (sistema de detección de intrusos) u otros sistemas, eligiendo la opción 2, Windows Meterpreter Reverse_TCP.

Seleccione el puerto 443 para que el tráfico parezca tráfico SSL. SET crea el documento PDF malicioso y establece el puerto.

Después de llevar a cabo estas acciones, SET le pregunta si quiere cambiar el nombre del PDF a uno más engañoso como `TechnicalSupport.pdf` y después le pide que cumplimente la información de los correos electrónicos tanto de entrada como de salida. Por último, SET envía un correo electrónico de aspecto profesional que intentará engañar al usuario para que abra el documento adjunto. En la figura 7.24 puede ver un ejemplo del aspecto del correo electrónico que recibe el objetivo.

Greetings,

Please view the latest status report.

Thanks,

Rich

---

template.pdf
70K View as HTML Download

Figura 7.24. *Un correo electrónico inofensivo con un sencillo archivo adjunto.*

Una vez enviado el correo, SET prepara el receptor y espera a que el objetivo abra el archivo. Cuando el objetivo hace clic en el PDF, el receptor responde manipulando el código malicioso entrante y dando al atacante acceso al ordenador de la víctima.

Sorprendentemente (o quizá no, dependiendo de sus perspectivas), todo esto se hace haciendo seis o siete veces clic en el ratón y otorga al auditor la libertad de centrarse en los aspectos más relacionados con la ingeniería social de estos ataques.

Éste es un ataque devastador porque explota un elemento de software cliente y muchas veces no hay ninguna indicación en pantalla de que esté sucediendo algo irregular. Éste es sólo uno de los muchos ataques que se pueden lanzar empleando SET.

Ataques de sitios Web

SET también permite al auditor clonar cualquier sitio Web y alojarlo localmente. El poder de este tipo de ataque es que le permite engañar a los usuarios para que visiten el sitio Web pretendiendo ser un desarrollador realizando algunos cambios o incluso empleando el truco de añadir o quitar una letra de la URL y dirigiendo a la gente al sitio clonado.

Una vez que la víctima se encuentra en el sitio Web clonado, se pueden lanzar distintas partes del ataque: recopilación de información, obtención de credenciales o explotación, son sólo algunas de ellas.

Para ejecutar este ataque en SET, debe elegir la opción 2, Website Attack Vectors (Vectores de ataque de sitios Web), del menú principal. Al elegir la opción 2 se le ofrecen varias opciones de ataque:

1. El ataque del Applet de Java (The Java Applet Attack Method).
2. La explotación del navegador de Metasploit (The Metasploit Browser Exploit Method).
3. El método de recopilación de credenciales (Credential Harvester Attack Method).
4. El método del *tabnabbing* (Tabnabbing Attack Method).
5. El ataque del hombre entre dos aguas (Man Left in the Middle Attack Method).
6. Volver al menú anterior (Return to the previous menu).

Un ataque especialmente malintencionado es el que ofrece la primera opción, el ataque del Applet de Java. Básicamente, este ataque muestra al usuario una advertencia de seguridad de Java diciendo que la empresa X ha firmado el sitio Web y le pide al usuario que apruebe la advertencia.

Para llevar a cabo este ataque, elija la opción 1 y después la opción 2, Site Cloner (Clonador del sitio Web).

Una vez que elija la opción Site Cloner, le preguntará qué sitio Web quiere clonar. Aquí puede elegir lo que mejor le parezca: el sitio Web del cliente, el de un proveedor o un sitio Web gubernamental. La elección es suya. Como habrá imaginado, es fundamental elegir un sitio Web que tenga sentido para el objetivo.

En este ejercicio, imagine que ha clonado Gmail. Aparecerá lo siguiente en pantalla:

```
SET supports both HTTP and HTTPS
Example: http://www.estoesunsitiowebfalso.com
Enter the url to clone: http://www.gmail.com
[*] Cloning the website: http://www.gmail.com
```

```
[*] This could take a little bit…
[*] Infecting Java Applet attack into the newly cloned website
[*] Filename obfuscation complete. Payload name is: DAUPMWIAHh7v.exe
[*] Malicious java applet website prepped for deployment
```

Una vez que termina este proceso, SET le preguntará el tipo de conexión que quiere que se cree entre usted y la víctima. Para emplear una tecnología explicada en este libro, elija la consola inversa de Metasploit llamada Meterpreter.

SET le da la opción de codificar su contenido con diferentes codificadores. Esto le ayuda a evitar ser descubierto por sistemas antivirus.

Después, SET lanza su propio servidor Web integrado, aloja el sitio Web y prepara un receptor para detectar al objetivo cuando navegue por el sitio.

Ahora depende del auditor enviar un correo electrónico o realizar una llamada para atraer al objetivo hacia la URL. En última instancia, el usuario verá algo parecido a lo que se muestra en la figura 7.25.

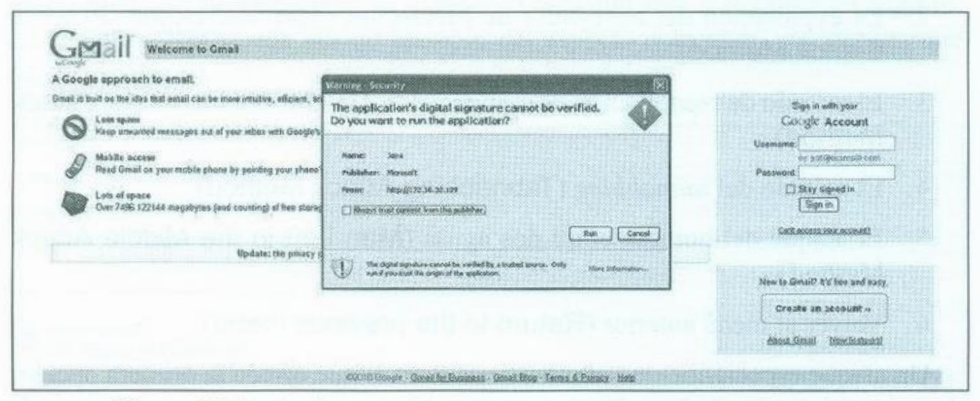


Figura 7.25. *¿Quién no se fiaría de un applet firmado por Microsoft?*

El resultado final es que al usuario se le muestra un *applet* de Java afirmando que el sitio Web ha sido firmado por Microsoft y que el usuario debe permitir que se ejecute el certificado de seguridad para poder acceder.

En el momento en que el usuario permite la certificación de seguridad, el atacante obtiene un *prompt* a su ordenador.

Otras características de SET

SET fue desarrollado por ingenieros sociales y pensando en ingenieros sociales; por lo tanto, el juego de herramientas que ofrece al usuario se basa en los ataques más comunes que necesitan llevar a cabo quienes se dedican a las auditorías de seguridad.

SET está en crecimiento y expansión continuos. En los últimos meses se ha logrado que SET pueda realizar otros ataques además de la clonación Web y el *phishing*; también alberga un generador de sistemas multimedia infecciosos. Con este generador, el usuario puede crear un DVD, CD o llave USB codificado con un archivo malicioso que puede dejarse en el edificio de oficinas del objetivo. Cuando se inserta en un ordenador, ejecuta el contenido malicioso y pone en peligro el ordenador de la víctima.

SET también puede crear un contenido sencillo y el puerto adecuado para él. Si el ingeniero social sólo necesita un EXE que sea una consola inversa que se conecte a sus servidores, puede llevarlo en una llave USB para emplearlo en una auditoría. Si se encuentra en una situación en la que necesita obtener el control remoto de un ordenador, puede insertar la llave USB y abrir el contenido. Esto le dará una conexión rápida a sus ordenadores.

Un nuevo vector de ataque es el llamado Teensy HID. Los dispositivos Teensy son pequeñas placas de circuitos programables que pueden insertarse en el teclado, el ratón u otros aparatos electrónicos que puedan enchufarse al ordenador.

SET tiene la capacidad de programar estos circuitos para que se comporten de cierta manera; son habituales los comandos para crear una consola inversa o preparar los puertos. Una de las características más novedosas de SET es la interfaz de la herramienta. Esto implica que un servidor Web alojará automáticamente SET en un sitio Web para una utilización más sencilla. La figura 7.26 muestra el aspecto de esta interfaz Web.

SET es una herramienta poderosa creada para ayudar al auditor a poner a prueba las vulnerabilidades de las empresas. El desarrollador de SET siempre está abierto a sugerencias y a colaboración para crear nuevos elementos para la herramienta para continuar creciendo y aumentar su popularidad. De nuevo, `www.social-engineer.org` ofrece una explicación clara de cada opción de menú para su revisión si quiere profundizar más en esta asombrosa herramienta. Continúe visitando tanto `www.social-engineer.org` como `www.secmaniac.com` para estar al día con las actualizaciones de SET.

Herramientas telefónicas

Una de las herramientas más antiguas de los ingenieros sociales es el teléfono. En la actualidad, con la telefonía móvil, la VoIP y los servidores telefónicos caseros, las opciones para utilizar esta herramienta han crecido considerablemente.

Debido a la proliferación del telemarketing, las presentaciones de ventas y la publicidad, el auditor de seguridad debe ser habilidoso para emplear el teléfono con éxito. A pesar de estas limitaciones, el uso del teléfono puede llevar a una empresa a una situación comprometida en un corto periodo de tiempo.

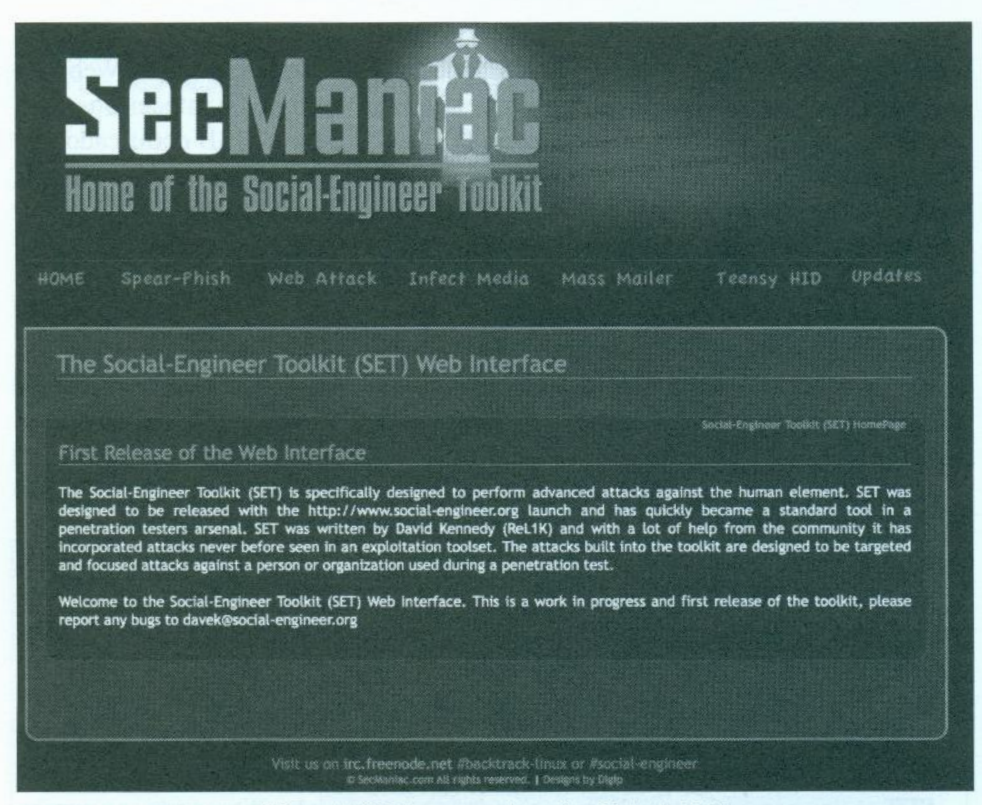


Figura7.26. *La nueva interfaz Web de SET.*

En esta era en la que todo el mundo tiene un teléfono móvil y mantiene conversaciones personales en el autobús, en el metro o en otros lugares públicos, el teléfono puede emplearse de muchas maneras diferentes. Las escuchas furtivas o las llamadas a los objetivos proporcionan nuevos vectores de ataque que no existían en el pasado. Con el número creciente de teléfonos *smartphone* y teléfonos con atributos de ordenadores personales, cada vez más gente guarda contraseñas, datos personales e información privada en sus teléfonos. Esta circunstancia otorga al ingeniero social la posibilidad de acceder al objetivo y a sus datos en muchas situaciones diferentes.

Además, al estar conectada 24 horas al día, la gente está más dispuesta a revelar información rápidamente si su interlocutor cumple ciertos "criterios" que lo hagan creíble. Por ejemplo, si la identificación de la llamada indica que la persona que está llamando lo hace desde la sede de una empresa, mucha gente revelará información sin exigir verificación alguna. Tanto el *smartphone* iPhone como el Android incluyen aplicaciones que pueden emplearse para falsificar la identificación de la llamada. Aplicaciones como SpoofApp (`www.spoofapp.`

com) permiten realizar llamadas que parezcan hechas desde cualquier parte del planeta a un coste relativamente bajo. Esto ayuda a darle credibilidad a su pretexto. La utilización del teléfono en las auditorías de seguridad puede dividirse en dos áreas diferentes: la tecnología que hay detrás de ella y la planificación de las llamadas.

Falsificación de la identificación de la llamada

La identificación de llamadas se ha convertido en una tecnología habitual tanto en los negocios como en los hogares. Sobre todo ahora, con la sustitución de los teléfonos de línea fija por teléfonos móviles, la identificación de llamadas es parte de la vida diaria. Como auditor de seguridad es importante ser consciente de este hecho y de las posibilidades que ofrece.

La falsificación de la identificación de llamadas consiste básicamente en cambiar la información que aparece en el visualizador del objetivo. En otras palabras, aunque esté haciendo la llamada desde un número, puede aparecer otro distinto en el identificador de llamadas del objetivo.

Una forma de utilizar esta información es utilizar el número de un proveedor con el que trabaja su objetivo. Si el ingeniero social averigua que el objetivo utiliza a la empresa X para darle asistencia técnica, puede buscar ese número y utilizarlo para que aparezca en el identificador de la llamada para concertar una cita. Con este método puede "localizar" llamadas desde:

- Una oficina externa.
- El interior de la oficina.
- Una empresa asociada.
- Una compañía de servicios (teléfono, agua, Internet, etc.).
- Un superior.
- Una empresa de transportes.

Por lo tanto, ¿cómo falsifica la llamada? Las siguientes secciones explican algunos de los métodos y equipos disponibles para falsificar números de teléfono.

SpoofCard

Uno de los métodos más populares es utilizar una tarjeta SpoofCard (www.spoofcard.com/). Para utilizar esta tarjeta, llama al número que le proporcionan en la tarjeta, introduce su número PIN, el número que quiere que visualice el receptor y el número al que quiere llamar.

Algunas características nuevas de SpoofCard le ofrecen la posibilidad de grabar la conversación telefónica y ocultar su voz para parecer un hombre o una mujer. Estas características aumentan su capacidad para ocultar el origen de la llamada y engañar al objetivo para que revele información.

Además, SpoofCard es muy fácil de utilizar, no necesita hardware o software extra, aparte de su teléfono, y ha demostrado su eficacia con miles de clientes. El único aspecto negativo de SpoofCard es su precio.

SpoofApp

Con tanta gente utilizando teléfonos *smartphone* como iPhone, Android o Blackberry, se ha producido una afluencia de aplicaciones diseñadas para falsificar la identificación de llamadas. SpoofApp utiliza tarjetas SpoofCard (vea la sección anterior) pero reúne todas sus características y las introduce como un paquete en su teléfono móvil.

En lugar de tener que llamar a un número gratuito, simplemente introduce el número al que quiere llamar en la aplicación, introduce el número que quiere que aparezca y SpoofApp le conecta con el objetivo mostrando ese número. Todo tan sencillo como pulsar un botón.

Asterisk

Si tiene un ordenador de sobra y un servicio de VoIP, también puede utilizar un servidor Asterisk para falsificar la identificación de llamadas. Encontrará más información sobre este método en `www.social.engineer.org/wiki/archives/CallerIDspoofing/CallerID-SpoofingWithAsterisk.html`. Un servidor Asterisk funciona de un modo muy parecido a SpoofCard, con la excepción del servidor que se utiliza para falsificar la identificación de la llamada. En este caso, el servidor es suyo. Esto es interesante porque le otorga mucha más libertad y no hay que temer un corte de línea o que se acaben los minutos de llamadas.

Los aspectos positivos de Asterisk son que es gratis, es fácil de utilizar, es flexible después de instalarse y el atacante tiene todo el control sobre él. Las desventajas más importantes son que se necesita un ordenador o una máquina virtual extra, que es necesario poseer ciertos conocimientos de Linux y que se necesita un proveedor de servicios VoIP.

Lo mejor de esta opción es que el ingeniero social posee toda la información sobre quién hace la llamada y sobre el destinatario de la misma. Los datos personales y de cuenta no están en las manos de terceras personas.

Emplear guiones

El teléfono es una de las herramientas favoritas de los auditores de seguridad. Proporciona anonimato y la habilidad de actuar sobre varios objetivos haciendo solamente ligeros cambios en el pretexto.

Un aspecto que se debe considerar es la utilización de guiones. Estos pueden ser un elemento importante para asegurar que se abordan todos los puntos necesarios; sin embargo, un guión no debe convertirse en un discurso aprendido de memoria palabra por palabra. Nada molesta más a un objetivo que tratar con una persona que da la sensación de estar leyendo un guión.

Después de escribir el guión debe practicarlo una y otra vez para sonar real, autentico y creíble.

Aquí es donde su sesión de recopilación de información cobra una importancia vital. Cuanto mejor sea la recopilación de información, más claro resultará el guión. A mí me resulta útil leer algunos datos sobre las aficiones e intereses del objetivo para utilizarlos para generar compenetración.

Cuando tenga toda la información preparada, puede ser útil trazar un plan de ataque. En el caso expuesto anteriormente, el del director general de la imprenta, tuve que desarrollar un esquema que me permitiera utilizar las partes clave de mi guión, los puntos importantes que quería tocar, así como notas para mí mismo como "habla con claridad", "no olvides sacar a relucir la obra de caridad", "ve despacio", etc., que me permitieron mantenerme concentrado durante la llamada.

Utilizar un guión o un esquema en lugar de un extenso manuscrito le ayudará proceder con fluidez y naturalidad y le otorgará libertad creativa cuando surjan imprevistos.

El teléfono todavía es una herramienta letal para el ingeniero social y, cuando se utiliza empleando los principios mencionados en este libro, conducen al auditor por el camino del éxito.

Descifrado de contraseñas

Otro tipo de herramientas que merece la pena mencionar le permiten perfilar a su objetivo y las contraseñas que puede emplear. Después de reunir toda la información que pueda sobre un objetivo, el siguiente paso es desarrollar un perfil. En ese perfil puede planificar algunos vectores de ataque que considere que pueden funcionar y también puede empezar a elaborar una lista de contraseñas potenciales para emplear en ataques de fuerza bruta. Desde la perspectiva de la herramienta, contar con una lista de posibles contraseñas puede ayudar a promover una modificación si tiene la opción. Esta sección presenta dos de los descifradores disponibles.

Las herramientas para descifrar contraseñas pueden ahorrarle horas e incluso días de trabajo. Cada año aumenta el número de personas que cae presa de ataques sencillos, a pesar de todas las advertencias que se hacen. Es increíble la cantidad de gente que revela todo tipo de información en Internet sobre ellos mismos, su familia y sus vidas. Combinando un perfil creado a partir del uso de los medios sociales de la persona, el resto de material que se encuentra en la red y empleando las herramientas explicadas, se puede perfilar la vida completa de una persona.

Uno de los motivos para que esto funcione tan bien es el modo en que la gente tiende a elegir sus contraseñas. Se ha demostrado que mucha gente utiliza la misma contraseña una y otra vez. Lo que es peor, la gente suele elegir contraseñas que son muy fáciles de adivinar sin tener habilidades especiales para ello.

Recientemente, BitDefender, una firma de seguridad en Internet, realizó un estudio que demostró este hecho. BitDefender analizó la utilización de contraseñas de más de 250.000 usuarios. Los resultados fueron sorprendentes: el 75 por 100 de ellos utilizaban las mismas contraseñas para sus cuentas de correo electrónico y todas sus cuentas en medios sociales. Estos datos son especialmente inquietantes teniendo en cuenta la historia reciente de cómo se reveló en un *torrent* la información personal de 171 millones de usuarios de Facebook. Puede leer la historia completa en `www.securityweek.com/study-reveals-75-percent-individuals-use-same-password-social-networking-and-email`.

En 2009, un hacker, con el alias de Tonu, realizó una investigación muy interesante. Sin malas intenciones se apropió de la URL de una red social muy popular, que había sido abandonada recientemente. Falsificó la página y durante un breve periodo de tiempo registró los intentos de la gente de entrar en la Web.

Puede ver los resultados en `www.social-engineer.org/wiki/archives/BlogPosts/MenAndWomenPasswords.html`.

Estos datos sorprenderán hasta a los profesionales de la seguridad más experimentados. De un total de 734.000 personas, 30.000 utilizaron su nombre como contraseña y casi 14.500 emplearon su apellido. Aunque estos datos son impactantes, lo que se descubrió a continuación fue absolutamente increíble. Las ocho contraseñas más utilizadas se indican en la tabla 7.1.

Tabla 7.1. *Contraseñas más utilizadas.*

Contraseña	Género	Número de usuarios
123456	M	17601
contraseña	M	4545
12345	M	3480

Contraseña	Género	Número de usuarios
1234	M	2911
123	M	2492
123456789	M	2225
123456	F	1885
qwerty	M	1883

¿17.601 hombres utilizaron como contraseña 123456? Impresionante.

Si esto no fuera lo suficientemente asombroso, Tonu señaló que más del 66 por100 de los usuarios de la lista emplearon contraseñas de seis u ocho caracteres de largo. Sabiendo que la mayoría de la gente utiliza contraseñas simples, resulta razonable utilizar una popular herramienta de crackeo, como Cain and Abel, mostrada en la figura 7.27, para descifrar contraseñas sencillas.

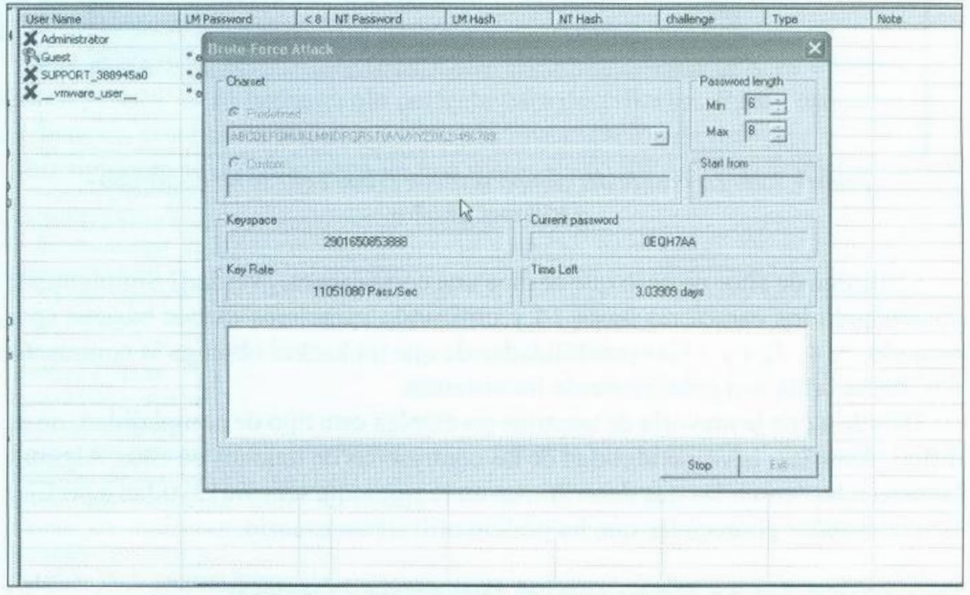


Figura 7.27. Sólo 3 días para descifrar una contraseña simple.

Observará que en el cuadro Time Left (Tiempo restante) dice 3,03909 días. Para la mayoría de los hackers, tres días es muy poco tiempo de espera para lograr acceder a un servidor. ¿Realmente tres días son tanto tiempo para esperar la contraseña del administrador?

Para que esta información cobre todo el sentido, observe la figura 7.28, que muestra la diferencia que habría si el mismo usuario empleara una contraseña de entre 14 y 16 caracteres con letras mayúsculas y minúsculas y caracteres no alfanuméricos.

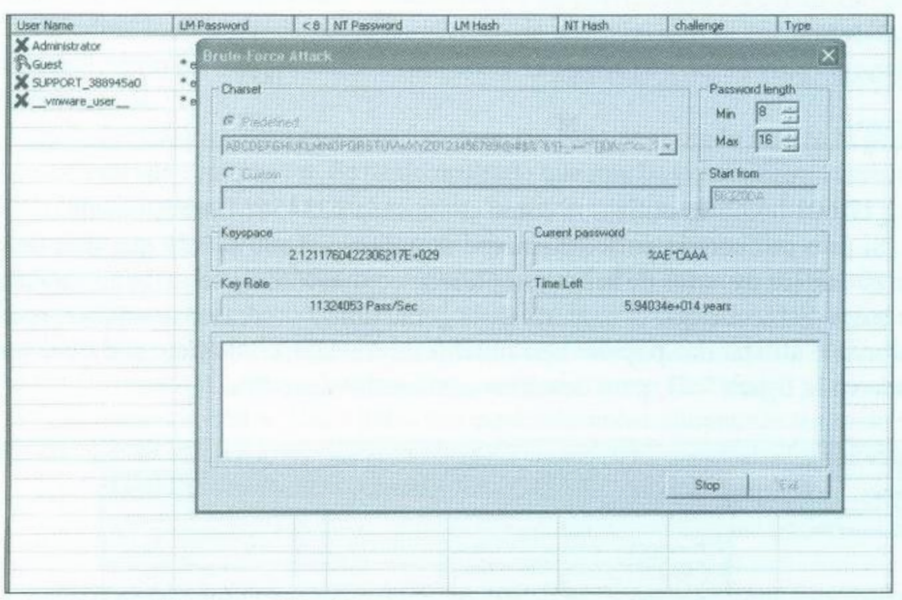


Figura 7.28. *La casilla del tiempo restante (Time Left) se ha disparado a trillones de años.*

5 trillones de años no es lo que se dice una corta espera, ¿verdad? Simplemente aumentando los caracteres hasta 14 y utilizando caracteres menos básicos (por ejemplo, *, &, $, % y ^) las posibilidades de que un hacker obtenga la contraseña por fuerza bruta son prácticamente inexistentes.

Debido a que la mayoría de usuarios no emplea este tipo de complejidad, no es difícil identificar la vulnerabilidad de las contraseñas de muchos de ellos. Algunas herramientas (como las que describimos en la siguiente sección) ayudan a perfilar las contraseñas potenciales que ha podido utilizar un usuario.

Common User Password Profiler (CUPP)

Perfilar a una persona es uno de los aspectos principales para tener éxito en una auditoría de seguridad. Como explicamos previamente, la investigación de Tonu muestra que de un total de 734.000 personas, más de 228.000 utilizaron sólo 6 caracteres en su contraseña. Más de 17.000 eligieron como contraseña "123456" y casi 4.600 eligieron la palabra "contraseña" como contraseña.

El Common User Password Profiler (Descifrador de contraseña habitual del usuario, CUPP) es una herramienta diseñada para descifrar contraseñas de forma sencilla.

Murgis Kurgan, también conocido como j0rgan, es el creador de esta asombrosa herramienta. Se ejecuta como un *script* en la distribución líder en pruebas de seguridad, BackTrack, y se puede descargar de www.social-engineer.org/cupps.tar.gz.

La forma más común de autentificación es la combinación de un nombre de usuario y una contraseña o frase secreta. Si ambos coinciden con los valores almacenados en una tabla, se autoriza la conexión al usuario. La seguridad de la contraseña es una medida de la dificultad que conllevaría adivinarla a través de técnicas criptográficas o la evaluación automática de archivos de valores alternativos.

Una contraseña vulnerable puede ser muy corta o estar compuesta tan sólo de caracteres alfanuméricos, haciendo que la descodificación sea muy sencilla. Una contraseña también es débil si puede ser fácilmente adivinada por alguien que esté realizando un perfil del usuario y utilice datos como el cumpleaños, un mote, una dirección, el nombre de una mascota o familiar o palabras habituales como "Dios", "dinero" o "contraseña".

Debido a que la mayoría de usuarios emplea contraseñas débiles y fáciles de adivinar, CUPP es la herramienta perfecta para descifrarlas. Puede utilizarse legalmente en pruebas de seguridad o para la investigación de delitos.

Lo siguiente es un corta/pega de una sesión de CUPP en BackTrack4:

```
root@bt4/pentest/passwords/cupp# ./cupp.py -i
[+] Introduzca la información sobre la víctima para crear un diccionario
[¡minúsculas!]
[+] Si no conoce toda la información, ¡simplemente presione enter cuando
se lo pida!
;)
> Nombre: John
> Apellido: Smith
> Apodo: Johnny
> Fecha de nacimiento: (DDMMYYYY; i.e. 04111985): 03031965
> Nombre de la mujer (marido): Sally
> Apodo de la mujer (marido): Sals
> Fecha de nacimiento de la mujer (marido): (DDMMYYYY; i.e. 04111985):
05011966
> Nombre del hijo: Roger
> Apodo del hijo: Roggie
> Fecha de nacimiento del hijo: (DDMMYYYY; i.e. 04111985): 05042004
> Nombre de la mascota: Max
> Nombre de la empresa: ABC Paper
> ¿Quiere añadir palabras clave sobre la víctima? Y/[N]: Y
> Por favor, introduzca las palabras separadas por coma. [i.e. hacker,
zumo, negro]: cristiano, cera, vendedor
> ¿Quiere añadir caracteres especiales al final de las palabras? Y/[N]: N
> ¿Quiere añadir números aleatorios al final de las palabras? Y/[N]: N
```

```
> ¿Escritura leet? (i. e. leet = 1337) Y/[N]: Y
[+] Creando el diccionario...
[+] Preparando la lista y eliminando duplicados...
[+] Guardando diccionario en John.txt, contando 13672 palabras.
[+] Ahora cargue con John.txt y ¡dispare! ¡Buena suerte!
```

Observe en la parte final que se ha creado un archivo de diccionario de 13.672 contraseñas utilizando la información introducida. El poder de este tipo de herramienta es que puede ahorrar mucho trabajo a la hora de averiguar contraseñas.

CeWL

Según sus creadores, CeWL es una aplicación Ruby que rastrea una URL dada en cierta profundidad, siguiendo vínculos externos si se desea, y elabora una lista de palabras que pueden utilizarse por crackers, como "Jack el destripador". Para más información sobre CeWL visite su Web en `www.digininja.org/projects/cewl.php`. Observe una sesión de CeWL en BackTrack4:

```
root@bt:/pentest/passwords/cewl# ruby cewl.rb
 --help cewl 3.0 Robin Wood (dninja@gmail.com)
(www.digininja.org)
Usage: cewl [OPTION] ... URL --help, -h: show help --depth x, -d x: depth
to spider to,
default 2 --min_word_length, -m: minimum Word length, default 3
--offsite, -o: let the
spider visit other sites --write, -w file: write the output to the file
--ua, -u user-
agent: user agent to send --no-words, -n: don't output the wordlist
--meta, -a file:
include meta data, optional output file --email, -e file: include email
addresses,
optional output file --meta-temp-dir directory: the temporary
directory,default /tmp -v:
verbose URL: The site to spider.

root@bt:/pentest/password/cewl# ./cewl.rb -d 1 -w pass.txt http://www.
targetcompany.com/about.php
root@bt:/pentest/password/cewl# cat passwords.txt |wc -l 430
root@bt:/pentest/password/cewl#
```

Utilizando CeWL sobre la empresa objetivo, la sesión ha generado 430 contraseñas potenciales con las que probar tan sólo de una página de su presencia en la Web.

CUPP y CeWL son sólo dos herramientas a su disposición para generar listas de contraseñas potenciales. Un ejercicio interesante consiste en ejecutar una de estas herramientas utilizando su propia información para comprobar si en la lista creada aparece alguna de las contraseñas que utiliza. Puede hacerle pensar para tomarse el tema de la seguridad de las contraseñas con mayor seriedad.

Resumen

Las herramientas son un aspecto muy importante de la ingeniería social, pero no hacen al auditor de seguridad. Una herramienta por sí sola es inútil, pero el conocimiento de cómo emplearla es de un valor incalculable.

Si una cosa queda clara en este capítulo es que la práctica lleva a la perfección. Ya sea empleando el teléfono, una herramienta de software, la Web u otros artilugios de espionaje, la practica es la clave para el éxito. Por ejemplo, cuando utilice el teléfono, puede emplear tecnologías de falsificación o de cambio de voz, pero, aunque tener a su disposición toda esta tecnología es impresionante, si al hacer la llamada su discurso suena artificial y memorizado, nervioso o falto de preparación, se perderá la oportunidad y seguramente la credibilidad también. Este principio vuelve a la idea de ser muy versado en la técnica del pretexto. ¿Cómo hablaría la persona que va a interpretar? ¿Qué diría? ¿Qué conocimientos tendría? ¿Qué información pediría?

Ya sea utilizando una herramienta de software o una herramienta física o las dos, la clave reside en tomarse el tiempo necesario para aprender las ventajes e inconvenientes de cada característica de la herramienta.

Las herramientas pueden ahorrarle mucho tiempo en sus auditorías y también pueden ayudar a cubrir alguna posible carencia del auditor. Esta idea se hace evidente al analizar los casos prácticos del capítulo 8.

8. Estudio de casos prácticos: diseccionando al ingeniero social

La mejor seguridad se consigue a través de la formación.
Mati Aharoni

A lo largo de este libro hemos recorrido cada aspecto que conforma a un buen ingeniero social. Poner en juego la información contenida en estas páginas convertirá al auditor de seguridad en una fuerza a tener en cuenta.

En el colegio, los estudiantes repasan la historia para aprender lo que conviene hacerse y lo que no. La historia es una buena herramienta para educarnos y enseñarnos lo que funcionó en el pasado y por qué lo hizo. Nos dice hacia dónde vamos y cómo llegar hasta allí.

La historia de la ingeniería social funciona del mismo modo. Desde que existen los negocios, hay estafadores y ladrones. Y, desde entonces, hay gente que ha dedicado su vida a ayudar a protegerse de estas acciones perjudiciales.

Siempre es complicado explicar los aspectos de los ataques de ingeniería social profesionales, porque o bien fueron realizados de forma ilegal o bien no pueden discutirse abiertamente debido a obligaciones contractuales. Por suerte, Kevin Mitnick (experto en seguridad informática y auditor famoso en el mundo entero) ha publicado muchas de sus experiencias para nuestro disfrute. Muchas de las historias de este capítulo están extraídas de su libro *The Art of Deception* (El arte del engaño).

He elegido dos de las historias más famosas de Mitnick y he incluido un breve resumen de la actuación de Kevin analizando qué aspectos de la ingeniería social utilizó y explicando lo que se puede aprender de dicha acción.

Después de diseccionar estos dos ataques, paso a hacer lo mismo con dos de mis propias experiencias, que demuestran la facilidad con la que puede obtener información y lo sencillo que resulta utilizar esta información para poner en situación de peligro a toda una empresa. Por último, revelo dos historias de alto secreto cuyas fuentes no pueden ser mencionadas, pero de las que, como verá, se puede aprender mucho. Lo que pretendo lograr es mostrarle lo peligrosa que puede resultar hasta la información aparentemente más insignificante y lo devastadora que puede ser en manos de un ingeniero social experimentado. Al mismo tiempo, aprenderá cómo se puede aprender de los éxitos y los fracasos pasados para mejoras sus propias habilidades. Empecemos con el primer caso práctico.

Estudio de caso de Mitnick 1: el pirateo de DMV

Kevin Mitnick es uno de los ingenieros sociales más famosos a nivel mundial. Ha llevado a cabo algunas de las explotaciones de vulnerabilidades más audaces y célebres del mundo. Aquí explicamos una de ellas.

En ocasiones, un carné de conducir puede venir muy bien para sonsacarle información a la gente. Poseer el número de carné del objetivo puede conducir al atacante a obtener todo tipo de información personal. Sin embargo, no existe un servicio gratuito al que recurrir para acceder a este tipo de datos. Un auditor o un investigador privado debe hacer todo lo posible para obtener y utilizar esta información con un objetivo.

En su libro *The Art of Deception*, Kevin Mitnick incluye una historia a la que denomina *The Reverse Sting* (La picadura inversa). En las siguientes secciones proporcionamos los antecedentes y el análisis de esta historia.

El objetivo

En una de las mejores historias de Mitnick, describe cómo "Eric" pretendía utilizar el servicio privado del Department of Motor Vehicles (DMV, Departamento de vehículos a motor) y el sistema de pólizas para conseguir los números del permiso de conducir de la gente. Necesitaba obtener este tipo de información a menudo. Eric tenía un método para lograrlo, pero temía que un exceso de llamadas telefónicas acabara por hacer que perdieran su efecto o que alertaran a la policía.

Necesitaba un nuevo método para acceder a la red del DMV y con el conocimiento del funcionamiento del DMV, sabía exactamente cómo hacerlo. Su objetivo era doble: tanto el DMV como la policía le ayudarían, por supuesto sin saberlo, a lograr su meta de obtener esta información.

La historia

Eric sabía que el DMV podía revelar información privilegiada a las aseguradoras, a investigadores privados y a algunas otras organizaciones. Cada sector tiene acceso solamente a cierto tipo de datos.

Una aseguradora puede obtener información diferente a un investigador, mientras que un agente del orden puede obtenerla toda. La meta de Eric era conseguirla toda.

Obtener un número de teléfono inédito del DMV

Eric dio una serie de pasos que pusieron de manifiesto sus excelentes habilidades como ingeniero social. Primero, hizo una llamada al servicio de información telefónica y pidió el número de la sede del DMV. Por supuesto, lo que obtuvo era el número público de la empresa pero él quería algo que le permitiera llegar más lejos.

Entonces llamó a la oficina del *sheriff* y pidió hablar con Teletype, la oficina donde se reciben y envían las comunicaciones con otras oficinas de las fuerzas del orden. Una vez que contactó con el departamento de Teletype, pidió el número que las autoridades utilizan para comunicarse con el DMV.

No sé que opinará usted, pero daba la impresión de que esta táctica fracasaría. Y casi lo hace:

"¿Quién es usted?", le preguntaron.

Tuvo que pensar con rapidez y contestó: "Soy Al. Llamaba al 503-555-5753".

Lo que hizo fue dar un número al azar con el mismo prefijo local e inventando los últimos dígitos. Después guardó silencio. El agente hizo algunas suposiciones:

- Era un interno y ya tenía el número privado (Teletype).
- Tenía prácticamente todo el número del DMV.

Convencido de estos dos datos, el agente dio por hecho que Eric estaba autorizado y le dio el número. No obstante, Eric quería más de un número; quería todos los que pudiera conseguir.

Para conseguir su meta necesitaría un ataque aún más profundo: uno a varios niveles y polifacético, con varias posibilidades. Tendría proporciones épicas.

Obtener acceso al sistema telefónico del estado

Eric llamó al número que le dieron del DMV. Le dijo al representante del departamento que era de Nortel (una empresa norteamericana de telecomunicaciones) y que necesitaba hablar con un técnico porque estaba trabajando con DMS-100, un interruptor de velocidad muy utilizado.

Cuando habló con el técnico le explicó que trabajaba en el centro de asistencia técnica de Nortel de Texas y que estaba actualizando todos los interruptores. El proceso se haría a distancia, por lo que el técnico no tendría que hacer nada más que proporcionar los números telefónicos de entrada de los interruptores para que Eric pudiera realizar las actualizaciones directamente desde el centro de asistencia técnica.

La historia resulta perfectamente creíble, por lo que el técnico accedió, dándole a Eric toda la información que pedía. Armado con esta información, Eric podía ahora llamar directamente a uno de los interruptores telefónicos estatales.

Conseguir contraseñas

El siguiente obstáculo era tan significativo que podía haber echado a perder todo el ataque: debía obtener algunas contraseñas. Los interruptores de Nortel que utilizaba DMV estaban protegidos por contraseña. Gracias a experiencias anteriores utilizando los interruptores de Nortel, Eric sabía que la empresa empleaba una cuenta de usuario predeterminada, NTAS. Eric marcó varias veces probando las contraseñas estándar que encontró:

- NTAS: fallo.
- Nombre de cuenta: fallo.
- Ayuda: fallo.
- Conexión: fallo.
- Actualización: ÉXITO.

Vaya, ¿en serio? Sí, la contraseña era "actualización". Ahora Eric tenía control total sobre el interruptor y todas las líneas conectadas a él. Averiguó cuáles eran las líneas telefónicas que correspondían a su objetivo. Rápidamente, descubrió que había 19 líneas que conectaban con el mismo departamento.

Después de estudiar el funcionamiento interno del interruptor, descubrió que estaba programado para buscar entre las 19 líneas hasta encontrar una que no estuviera ocupada. Escogió la línea 18 e introdujo el código de desvío estándar que añadía un comando de desvío de llamada a esa línea telefónica.

Eric compró un teléfono móvil barato de prepago del que podría deshacerse fácilmente. Introdujo ese número como el número al que debía desviarse la llamada cuando sonara la línea 18. Básicamente, cuando el DMV tuviera ocupadas 17 líneas, la siguiente llamada no entraría en el DMV sino en el teléfono móvil de Eric.

No pasó mucho tiempo hasta que esto empezó a suceder. Sobre las 8 de la mañana siguiente el teléfono móvil empezó a sonar. En todas las ocasiones se trataba de un oficial de policía pidiendo información sobre alguna persona. Allí donde estuviera, interceptaba llamadas de la policía: en casa, en el almuerzo, en el coche; no importa donde estuviera, en cada ocasión se hacía pasar por un representante del DMV.

Resulta bastante graciosa la parte del libro en la que Kevin describe cómo solían desarrollarse las llamadas:

Sonaba el telefono y Eric decía: "DMV, ¿en qué puedo ayudarle?".

"Aquí el detective Andrew Cole".

"Buenos días, detective, ¿qué puedo hacer por usted?".

"Necesito un Soundex del permiso de conducir 005602789".

"Por supuesto, espere un momento mientras abro el registro". Mientras simulaba trabajar con el ordenador Eric hacía un par de preguntas: "Detective Cole, ¿cuál es su agencia?".

"Condado de Jefferson".

Entonces Eric continuaba preguntando: "¿Cuál es su código de solicitante?". "¿Cuál es su número de permiso de conducir?". "¿Cuál es su fecha de nacimiento?".

Cuando el agente proporcionaba toda esta información, Eric pretendía estar verificando los datos. Después, fingía la confirmación y le preguntaba los detalles de su llamada. Entonces, simulaba buscar la información y decía: "Mi ordenador se ha vuelto a colapsar. Lo siento, detective, mi ordenador lleva dando problemas toda la semana. ¿Le importaría volver a llamar para que le atienda otro empleado?".

Seguramente esto resultaba un poco molesto para el agente, pero servía para atar todos los cabos sueltos. En el proceso, Eric se había hecho con la identidad de ese agente. Podría utilizar esa información para muchas cosas, pero sobre todo para obtener información del DMV cuando lo necesitara.

Llevó a cabo esta recopilación de información del DMV durante unas horas y después desactivó el desvío de llamadas: ahora tenía en su poder una buena cantidad de información muy valiosa.

Durante los meses siguientes a este ataque, Eric pudo volver a llamar, activar el desvío de llamadas, recopilar cierta cantidad de datos de un agente, desactivar el desvío de llamadas y después emplear esos credenciales policiales para obtener información de permisos de conducir que podía vender a investigadores privados u otras personas que no preguntarían cómo había conseguido esa información.

Aplicación del ámbito conceptual de la ingeniería social en el ataque del DMV

En esta historia, Kevin identificó algunas de las cosas que hizo Eric y algunas de las actitudes que le llevaron al éxito, como ser capaz de no sentirse incómodo o intimidado por hablar con la policía y saber manejarse en áreas desconocidas.

También puede identificar los conceptos de la ingeniería social que empleó Eric y cómo lo hizo.

Por ejemplo, el primer paso en una auditoría o ataque es la recopilación de información. En esta historia, puede comprobar que Eric tuvo que aplicarse en esta área antes relanzar su ataque. Sabía mucho sobre el sistema telefónico, el modo en que trabajaba el DMV y el funcionamiento general del proceso que quería infiltrar. No estoy seguro de hace cuánto tiempo tuvo lugar este ataque, pero hoy en día un ataque de este estilo es aún más sencillo gracias a Internet. Es una mina de oro para la recopilación de información. Hace un par de años alguien descubrió un sistema para piratear un cajero automático y en cuestión de semanas había manuales en Internet explicando paso por paso cómo realizar el ataque.

Además, tal como mencionamos previamente en este libro, elegir un pretexto que tenga que ver con las cosas que hace o ha hecho en su vida real aumenta las probabilidades de éxito. La razón es que, al ser un pretexto más "realista", resulta más sencillo recopilar información y provocar la brecha en el objetivo. Eric demostró tener un gran conocimiento de este campo.

Como recordará, el siguiente punto del ámbito conceptual de la ingeniería social son las maniobras de obtención de información o, lo que es lo mismo, ser capaz formular preguntas que le permitan acceder a la información o al lugar que desea. Eric sonsacó la información con maestría. Al teléfono con la policía fue capaz de demostrar ser quien pretendía ser. Conocía la jerga y preguntas rutinarias que debía formular. Si no hubiera hecho esas preguntas podría haber hecho saltar alguna alarma en algún agente. Ése es el verdadero poder de las tácticas para sonsacar información.

Eric supo enseguida que debía conseguir ciertos números de teléfono para lanzar su ataque. En lugar de intentar explicar por qué necesitaba cierta información, utilizó la presunción, tal como se explica en el capítulo 3, e hizo preguntas que básicamente afirmaban: "Merezco estas respuestas, así que dígame lo que le pregunto". Éste es otro ejemplo del poder de las maniobras de obtención de información; puede aprender mucho analizando estos métodos con detenimiento.

La mayoría de los ataques exitosos también incluyen una gran cantidad de pretexto. Este caso no es una excepción. Eric tuvo que desarrollar varios pretextos en este ataque. Tuvo que cambiar de marcha varias veces para llegar a su meta.

Por muy impresionante que le parezca que Eric se hiciera pasar por un agente del orden (y haciéndolo muy bien, además), tenga en cuenta que esta práctica es absolutamente ilegal en muchos países. Puede aprender mucho del procedimiento y los métodos empleados por Eric, pero tenga cuidado si decide aplicarlos. Incluso en una auditoría profesional, es ilegal hacerse pasar por un agente del orden.

La lección es ésta: conozca sus leyes locales y asuma las consecuencias. A pesar de ser ilegal, la actitud de Eric en este ataque es digna de analizar. Se mantuvo sereno en todo momento. Cuando puso en juego el pretexto del agente del DMV fue capaz de sonsacar una información que pudo utilizar como prueba. Cuando utilizó el pretexto del policía, su conducta, su voz y sus frases ayudaron a consolidarlo. Realizar estos cambios puede ser muy difícil para ciertas personas, por lo que lo mejor es practicar antes de emplearlas en una auditoría.

Los pretextos de Eric fueron sólidos e hizo un trabajo excepcional manteniendo su posición, sobre todo cuando tuvo que actuar como un agente del DMV y recibir llamadas reales de la policía. Podía haberse salido del papel fácilmente, pero consiguió aguantar la presión notablemente.

Muchas de las técnicas relacionadas con los aspectos psicológicos de la ingeniería social, como los movimientos oculares y las microexpresiones, no se emplearon en este ataque porque éste se realizó mayoritariamente por teléfono. No obstante, Eric tuvo que valerse de ciertos aspectos del ámbito conceptual, como la creación de compenetración, la programación neurolingüística y las modalidades sensoriales.

Eric demostró crear compenetración con mucha naturalidad. Fue amable y estuvo muy relajado en todo momento, dando la sensación de no temer los imprevistos y fue capaz de mostrarse confiado en sus habilidades. Moduló su voz y su conversación de un modo que la persona al otro lado del teléfono no tenía ningún motivo para no confiar en él y creerle.

Eric empleó tácticas de interrogatorio y entrevista impresionantes, incluso con agentes de la ley que tienen experiencia en este tipo de maniobras. Utilizó estas tácticas de forma tan satisfactoria que no fue descubierto y obtuvo toda la información que quiso.

También dio la sensación de tener un gran conocimiento y mucha habilidad para utilizar tácticas de persuasión. Una de las más llamativas en este ataque tuvo lugar cuando le pidió al agente de policía que volviera a llamar para hablar con otro empleado del DMV. Es probable que esto fuera molesto para el policía, pero la clave estuvo en que Eric le "dio" algo al agente "antes". Esto es: "verificó" los datos que necesitaba el oficial y, cuando se suponía que le iba a entregar la información final, es cuando su "ordenador" se bloqueó.

Aplicando algunas de las reglas de la influencia, Eric consiguió fácilmente que los agentes se plegaran a sus deseos.

Íntimamente relacionado con la utilización del pretexto, Eric empleó el encuadre con eficacia. Para refrescar su memoria, el encuadre consiste en alinear al objetivo con su línea de pensamiento posicionándose de tal manera que usted y sus argumentos le resulten creíbles. Es una pieza importante del puzle del pretexto que hace que destaque y consiga realmente demostrar al objetivo que es quien dice ser.

Los pretextos de Eric fueron buenos y creíbles, pero lo que realmente hizo que funcionaran fue los encuadres que utilizó. Su encuadre varió dependiendo de con quién estaba hablando.

En un momento dado, tuvo que lograr que el agente le proporcionara el número de Teletype; en otra llamada tenía que hacerse pasar por un experimentado empleado del DMV.

Eric ganó mucha credibilidad al utilizar el encuadre para asumir que conseguiría la información que estaba pidiendo, sin mostrar temor en el proceso y formulando las preguntas confiando en que le "debían" una respuesta.

Todas estas actitudes lograron que el objetivo aceptara su pretexto y contestara con naturalidad.

Como puede ver, se puede aprender mucho analizando el ataque de Eric. Uno debe asumir que o Eric practicó mucho todos estos métodos o realizó algunos ensayos generales para saber todo lo que sabía sobre los sistemas internos implicados en el ataque.

Los métodos de Eric funcionaron y tuvieron éxito, pero yo hubiera tomado un par de precauciones extra. Por ejemplo:

- Cuando estaba recibiendo llamadas dirigidas al DMV, me hubiera asegurado de desviar el número solamente cuando estuviera en la "oficina". Hubiera preparado un lugar para que funcionara como oficina, con algunos sonidos de oficina de fondo y hubiera tomado medidas para anotar toda la información necesaria para evitar que una camarera o un amigo estropearan mi acción.
- Aunque un teléfono deshechable es una buena idea para evitar ser rastreado, otra técnica consiste en desviar el número a un número de Google Voice o Skype. Tiendo a no confiar en la señal de los teléfonos móviles y nada hubiera sido más desastroso para el ataque que tener mala cobertura o que la llamada se cortara.

Aparte de estos puntos, no se puede mejorar mucho más este ataque. Eric realizó un trabajo excelente asegurándose de obtener un buen resultado utilizando muchas de las habilidades del ámbito conceptual de la ingeniería social para lograr su meta.

Estudio de caso de Mitnick 2: el pirateo de la administración de la Seguridad Social

Mitnick menciona a un hombre al que llama Keith Carter, un investigador privado de dudosa reputación contratado para investigar a un hombre que estaba escondiendo fondos a la que pronto sería su ex mujer. Ella había financiado la empresa de su marido, que a la larga se convirtió en una compañía multimillonaria.

El divorcio estaba preparado pero los abogados de la mujer querían encontrar los "activos escondidos". Este ataque es interesante porque, al igual que en el primer caso, la historia sigue un método muy turbio de recopilación de información.

El objetivo

El objetivo era encontrar los activos del marido, "Joe Johnson", pero ése no fue el objetivo empleado para este ataque. Para obtener información sobre Joe, el investigador privado, Keith, tuvo que piratear la Administración de la Seguridad Social (SSA, *Social Security Administration*).

Esta situación se presenta a menudo en una auditoría de seguridad. Esta sección aborda algunos de los métodos que empleó para lograr su meta, pero baste decir que piratear la SSA es una situación muy delicada. Según se vaya desarrollando la historia, comprobará lo peligroso que resultó este ataque concreto.

La historia

Joe Johnson estaba casado con una mujer muy rica. Se sabía que había invertido decenas de miles de dólares del dinero de ella en uno de sus proyectos. Este proyecto creció hasta convertirse en una organización multimillonaria.

El matrimonio no funcionó y decidieron divorciarse. Durante el proceso de divorcio, la señora Johnson se dio cuenta de que su marido estaba escondiendo dinero para que no formara parte del acuerdo de separación.

La señora Johnson contrató a Keith, el investigador privado de ética cuestionable, al que no le importaba cruzar la frontera entre lo legal y lo ilegal para obtener la información que buscaba.

Cuando Keith se sentó a analizar el caso, decidió que un buen punto de partida sería la Administración de la Seguridad Social. Pensó que si lograba hacerse con el historial de Joe podría detectar algunas discrepancias y dar el caso por cerrado.

Su intención era llamar a los bancos de Joe, las firmas financieras y sus cuentas en paraísos fiscales, haciéndose pasar por Joe. Para lograrlo necesitaba cierta información detallada, que fue lo que le condujo a la idea de atacar la oficina de la Seguridad Social.

Keith empezó reuniendo información básica. Se conectó a Internet y encontró una guía que describía el funcionamiento interno de la SSA y su terminología y jerga. Cuando estudió bien esta información y tuvo dominada la jerga llamó al número público local de la oficina de la Seguridad Social. Pidió que le pusieran con el departamento de reclamaciones. La conversación discurrió del siguiente modo:

"Hola, soy Gregory Adams, de la oficina del distrito 329. Verá, estoy buscando al perito que lleva un número de cuenta terminado en 6363 porque el número que tengo es de un fax".

"Ah, es Mod 3, el número es...".

¿En serio? ¿Así de fácil? En un momento consiguió el número de la oficina interna, un dato que normalmente no se proporciona al público. Ahora empieza la parte complicada.

Tenía que llamar a Mod 3, cambiar su pretexto y obtener información útil sobre Joe. Llegó el jueves y parecía que Keith tenía el plan bien trazado. Descolgó el teléfono y marcó el número de Mod 3:

"Aquí Mod 3, soy May Linn Wang".

"Señora Wang, soy Arthur Arondale, de la oficina del inspector general. ¿Puedo llamarla May?".

"Es May Linn", contesta ella.

"De acuerdo, May Linn, esto es lo que sucede. Tenemos un chico nuevo en la oficina que no tiene ordenador todavía. Está trabajando en un proyecto importante y está utilizando mi ordenador. ¡Por el amor de Dios! Somos el gobierno de Estados Unidos y dicen que no tienen presupuesto suficiente para comprar un ordenador nuevo para este chico. Y ahora mi jefe dice que me estoy retrasando y que está harto de excusas, ya sabes".

"Ya veo a lo que se refiere".

"¿Puede ayudarme con una consulta rápida en MCS?", preguntó, dando el nombre del sistema informático utilizado para buscar información sobre contribuyentes.

"Por supuesto, ¿qué necesita?".

"Lo primero que necesito es que haga un *alphadent* de Joseph Johnson, fecha de nacimiento 7 de abril de 1969". *Alphadent* quiere decir que el ordenador hace una búsqueda alfabética de una cuenta por nombre del contribuyente, identificado posteriormente por fecha de nacimiento.

"¿Qué necesita saber?".

"¿Cuál es su número de cuenta?", pregunta Keith (lo que está pidiendo es el número de la Seguridad Social de Joe).

Entonces ella se lo lee.

"Muy bien. Ahora necesito que haga un *numident* sobre ese número de cuenta". *Numident* es parecido a *alphadent*, pero la búsqueda es numérica en lugar de alfabética. De esta manera, Keith está solicitando que le proporcione información básica del contribuyente. May Linn respondió proporcionándole el lugar de nacimiento del contribuyente y el nombre de sus padres. Keith escuchó pacientemente mientras le decía también el mes, el año y el lugar en que fue expedido el número de la Seguridad Social de Joe.

Entonces Keith solicitó una "declaración detallada de ingresos".

"¿De qué año?".

"Año 2001".

May Linn dijo: "El total son 190.286 euros y el pagador es Johnson MicroTech".

"¿Algún otro pagador?".

"No".

"Muchas gracias", dijo Keith. "Ha sido muy amable".

Entonces Keith intentó quedar en llamarla cada vez que necesitara información y no "pudiera acceder a su ordenador", empleando uno de los trucos favoritos de los ingenieros sociales, que consiste en intentar establecer una conexión para poder acudir siempre a la misma persona, evitando de esta manera la molestia de tener que encontrar una nueva marca en cada ocasión.

"La próxima semana imposible", dijo ella, porque se iba a Kentucky a la boda de su hermana. Pero en cualquier otra ocasión haría lo que pudiera por ayudarle.

En este punto daba la sensación de que la meta estaba prácticamente alcanzada. Keith tenía toda la información que se había propuesto obtener y ahora sólo era cuestión de llamar a los bancos, lo cual, armado con la información de la que ahora disponía, sería una tarea mucho más sencilla.

Un ataque realmente impresionante y muy bien ejecutado.

Aplicación del ámbito conceptual de la ingeniería social en el ataque de la SSA

El ataque de la SSA recién explicado deja con la boca abierta y los ojos abiertos de par en par. Puede aprender mucho de este ataque, porque emplea muchos elementos del ámbito conceptual de la ingeniería social.

Keith inició el ataque con la recopilación de información. Probablemente ya esté cansado de oírme repetir lo mismo una y otra vez, pero tener información es la clave en cualquier auditoría o ataque. Cuanta más posea, mucho mejor.

Al principio, Keith encontró una información increíble en la Web, que, asombrosamente, aún sigue *on-line* en `https://secure.ssa.gov/apps10/poms.nsf/`.

Este vínculo le dirige a un manual *on-line* de Operación de Programas de la Administración de la Seguridad Social. Contiene abreviaturas, jerga e instrucciones, así como los datos que los empleados de la SSA están autorizados a proporcionar a las autoridades. Con esta información en el bolsillo, Keith sabía lo que tenía que preguntar, cómo preguntarlo para parecer alguien del sector, además de saber qué tipo de peticiones harían saltar las alarmas.

Aunque este vínculo proporcionaba una buena cantidad de información, decidió ir un paso más allá en su recopilación de información utilizando el pretexto de un empleado de la oficina general de inspección para llamar a su oficina local de la SSA. Utilizar su oficina local para obtener los números internos que necesitaba para completar su pretexto fue un movimiento muy astuto y original.

Keith cambió de pretexto un par de veces y lo hizo con maestría. Fue capaz de obtener mucha de la información que necesitaba utilizando el manual *on-line* de la SSA para plantear las preguntas adecuadas. Este manual se convirtió en el arma soñada para obtener información. Empleando el lenguaje y las palabras adecuadas, sonaba como si ése fuera su ámbito profesional. Desarrolló compenetración y un encuadre que respaldó su pretexto a la perfección. Crear compenetración no es tarea fácil, pero lo hizo muy bien y de un modo que demuestra que tenía mucha práctica con esta técnica. Utilizó muchas tácticas de persuasión para asegurarse de que el objetivo se sintiera cómodo y relajado. Por ejemplo, combinó el compromiso y la reciprocidad con mucha destreza. Cuando consiguió poner a May Linn de su parte explicando la falta de equipo y de apoyo por parte de sus superiores, ella sintió el compromiso de ayudarle.

También empleó frases y palabras clave que provocaban empatía y a la vez demostraban su posición de autoridad; frases como "mi jefe está harto" indican que tiene problemas y que May Linn puede salvarle. La gente siente la obligación moral de ayudar a quienes lo necesitan. Poca gente es capaz de ignorar a alguien que le pide ayuda y May Linn no es una de esas personas. Se sintió obligada, no sólo a ayudar, sino a hablarle a Keith de sus planes personales.

En definitiva, Keith empleó un buen número de las habilidades más importantes de la ingeniería social que no implican presencia física.

El hecho de que los sistemas gubernamentales sean gestionados por personas es lo que los hace vulnerables a este tipo de ataques. Ésta no es razón para inventar robots que hagan este trabajo; simplemente indica que muchos de estos sistemas

dependen demasiado de personas saturadas de trabajo y mal pagadas que no resultan demasiado difíciles de manipular.

Sinceramente, mejorar este ataque es complicado porque es un tipo de acción que yo nunca llevaría a cabo y porque Keith hizo un trabajo excelente aplicando los principios de la ingeniería social.

Hay tantas personas acostumbradas a que las traten mal y les griten que mostrarse un poco amables con ellas provoca que enseguida estén dispuestas a ayudar. Este ataque en particular, tal como se presenta en el libro de Mitnick *The Art of Deception*, demuestra lo vulnerables que son los sistemas que dependen de personas.

Estudio de caso de Hadnagy 1: el director general demasiado seguro de sí mismo

Mi experiencia con un director demasiado seguro de sí mismo es interesante porque este caballero consideraba que era inmune a cualquier intento de ataque por dos razones: primero, no utilizaba mucho la tecnología en su día a día y, segundo, pensaba que era demasiado listo y estaba suficientemente protegido como para no caer en lo que el llamaba "juegos tontos".

Sabiendo esto, su equipo interno de seguridad decidió pedirme que me concentrara en él en mi auditoría. Consideraban que si no superaba la auditoría sería más sencillo que aprobara la toma de medidas necesarias para mejorar su seguridad.

El objetivo

El objetivo era una imprenta de tamaño considerable que poseía algunas patentes y proveedores tras los que andaba su competencia. El equipo de tecnologías de la información y seguridad se percató de que la empresa era vulnerable y convenció al director de que era necesario realizar una auditoría. En una conferencia telefónica con mi socio, el director general, con cierta arrogancia, dijo que "piratearle a él sería poco menos que imposible, porque protegía esos secretos con su vida". Ni siquiera algunos de sus empleados más cercanos conocían todos los detalles.

Mi trabajo como auditor era infiltrarme en la empresa para acceder a uno de los servidores donde se alojaba la información de patentes y recuperarla. El problema, como dijo el director por teléfono, era que las contraseñas de los servidores estaban guardadas en su ordenador y nadie tenía acceso a él sin su permiso, ni siquiera el equipo de seguridad.

La historia

Aparentemente, la vía de entrada debía implicar al director general, lo que suponía un gran reto porque estaba alerta y preparado para un intento de ataque. Comencé del mismo modo que en todas mis auditorías: por la recopilación de información. Investigué la empresa utilizando recursos *on-line* y otras herramientas como Maltego. Conseguí reunir información como la localización de servidores, direcciones IP, direcciones de correo electrónico, números de teléfono, direcciones físicas, servidores de correo, nombres y títulos de los empleados y mucho más.

Por supuesto, organicé toda esta información de manera que fuera fácil de utilizar más adelante. La estructura del correo electrónico era importante porque cuando busqué en el sitio Web comprobé que era `nombre.apellido@empresa.com`. No pude localizar la dirección de correo electrónico del director general, pero muchos artículos mencionaban su nombre (digamos que se llamaba Charles Jones) y su título en su sitio Web. Éste era el tipo de información que un atacante estándar poco informado sería capaz de conseguir.

Empleando el formato `nombre.apellido@empresa.com`, intenté enviarle un correo electrónico, pero no funcionó. En ese momento me sentí bastante decepcionado, porque estaba seguro de que el método del correo electrónico conduciría a una buena cantidad de detalles jugosos.

Decidí probar un apodo de Charles, así que intenté con `chuck.jones@company.com`. ¡Éxito rotundo! Ya tenía un correo electrónico confirmado. Ahora debía verificar que se trataba del director general y no otro tipo con el mismo nombre.

Dediqué más tiempo a investigar con Google y Maltego para reunir toda la información que pudiera. Maltego tiene un transformador que permite buscar en un dominio cualquier archivo que sea visible para un motor de búsqueda normal.

Ejecuté el transformador sobre el dominio de la empresa y obtuve una increíble cantidad de archivos con la búsqueda. Maltego no se conforma con proporcionar nombres de archivo. Muchos archivos contienen metadatos, que son datos sobre las fechas, los creadores y alguna otra información golosa sobre el archivo. Pude comprobar que la mayoría de estos archivos habían sido creados por un tal "Chuck Jones". Gran parte del contenido de los archivos hablaba de él como el director general de la empresa.

Ésta era la confirmación que necesitaba. Durante la búsqueda, hubo un archivo que llamó especialmente mi atención: `FacturaAbril.xls`. Al leer el archivo descubrí que se trataba de una factura de un banco local de una operación en la que estuvo implicado Chuck. Tenía el nombre del banco, la fecha y la cantidad pero no sabía de qué tipo de evento se trataba.

Realicé una búsqueda muy rápida en el sitio Web del banco, pero como el evento había tenido lugar seis meses antes, no aparecía en la Web. ¿Qué podía hacer?

Decidí llamar al encargado de marketing del banco:

"Hola, soy Tom de la empresa X. Estoy intentado organizar los libros y tengo aquí una factura de abril de 3.500 euros en concepto de un patrocinio pero no veo el nombre del evento. ¿Puede decirme a qué corresponde esta factura?".

"Claro, Tom", dijo la chica con la que hablaba y escuché sonidos de ordenador. "Veo que se trata de la recaudación de fondos anual del banco para el tratamiento del cáncer infantil. Formáis parte del Modelo de Plata".

"Muchas gracias; soy nuevo en la empresa y me ha venido muy bien tu ayuda. Hablamos pronto".

Empezaba a formarse ante mí la posibilidad de un vector de ataque que podría emplear, pero necesitaba investigar más y tenía que planificar con mucho cuidado una llamada telefónica.

Encontré algunos artículos en Internet que hablaban de este evento para recaudar fondos y de todas las empresas que habían colaborado económicamente en la investigación para el tratamiento del cáncer infantil. Además, cuanto más profundizaba en mi investigación sobre el director general, más datos descubría sobre él. Conseguí el nombre de sus padres y hermanas, fotografías de sus hijos que tenía en Facebook, la iglesia a la que iba cuando vivía con sus padres, una reseña que escribió sobre su restaurante favorito, su equipo preferido y el de su hijo mayor, la universidad a la que asistió, el colegio en el que estudiaban sus hijos, etc.

Quería averiguar por qué la empresa donaba dinero a esta causa. Muchos ingenieros sociales malintencionados se aprovechan de los sentimientos de los demás y sabía que era posible que tuviera que recurrir a esa técnica, así que me proponía averiguar si estas donaciones tenían que ver con que alguno de sus hijos tuviera cáncer.

Llamé por teléfono al director de marketing de la empresa:

"Hola, soy Tom de la empresa X. El First National Bank de la ciudad nos ha encargado llamar a todas las empresas que tomaron parte en la recaudación de fondos para el tratamiento del cáncer infantil. Me preguntaba si podría dedicarme unos minutos de su tiempo para contestar a unas preguntas".

"Por supuesto", dijo Sue, la directora de marketing.

"Sue, veo que formasteis parte de nuestro Modelo de Plata en abril. ¿Consideras que la campaña que se realizó cumplió las expectativas en relación al dinero invertido?".

"Bueno, ésta es una actividad que realizamos todos los años y la verdad es que atraemos bastante atención de la prensa local. Creo que como parte del Modelo de Plata podría estar bien tener algo más de presencia en el sitio Web".

"Estupendo; tomo nota. Todos los años, es cierto, veo que participan en esta causa anualmente. A nivel personal me gustaría preguntarte, con tantos eventos de recaudación de fondos, ¿por qué habéis elegido éste precisamente?".

"Chuck siempre se ha centrado en esta obra. Es nuestro director general, creo que alguien de su familia ha tenido que enfrentarse a la enfermedad".

"Dios mío; lo siento. ¿No será uno de sus hijos, verdad?".

"No, creo que es un sobrino o un primo. La verdad es que nunca hablamos de ello".

"Bueno, quiero que sepas que agradecemos mucho vuestra colaboración".

Terminé con algunas preguntas más y después lo dejé, dándole las gracias por su tiempo.

Ya tenía la información que necesitaba. No era uno de sus hijos quien padecía cáncer. De nuevo sabía que esto no detendría a un ingeniero social malicioso, pero sentía mucha curiosidad. Con esta información estaba preparado para lanzar mi ataque.

Sabía que el director era de Nueva York y que su restaurante favorito era un local llamado Domingoes. Solía llevar a sus hijos a un partido de béisbol y después iban a comer a este restaurante.

Había escrito un artículo sobre Domingoes en el que hablaba de sus tres platos favoritos. Por lo que había escrito en Facebook sabía que sus padres vivían cerca y que los visitaba a menudo.

Planeé un ataque en el que me hacía pasar por un recaudador de fondos para la investigación del cáncer. Con una pequeña donación se participaba en una rifa. El premio eran dos entradas para ver al equipo favorito del director y una cena gratis a elegir entre tres restaurantes, uno de los cuales era Domingoes.

Le haría creer que yo también era de Nueva York, aunque desde hacía poco tiempo, por si me preguntaba cosas que no sabía.

Mi meta final era que aceptara un PDF con código malicioso que me proporcionaría una consola inversa y me daría acceso a su ordenador. Si no utilizaba una versión de Adobe que me permitiera el acceso, intentaría convencerle para que se descargara un archivo comprimido y ejecutara un EXE que contendría el archivo malicioso.

Practiqué la conversación telefónica que mantendría mi pretexto, probé los archivos PDF y EXE y abrí Google Maps con la localización de Domingoes para poder hablar sobre la zona sin problemas. Cuando tuve preparado el ordenador, esperando el contenido de la víctima, estuve listo para realizar la llamada.

La hice sobre las cuatro de la tarde, porque había averiguado a través de la Web de la empresa que los viernes cerraban la oficina a las cuatro y media. Ya que yo no participé en la conversación telefónica que dio origen a esta auditoría (lo hizo mi socio), el director no podría reconocer mi voz.

"Hola, ¿podría hablar con Charles Jones?".

"Por supuesto, un momento, por favor". La voz al otro lado del teléfono sonaba cansada y me pasó con el director rápidamente.

"Hola, aquí Chuck".

"Hola, señor Jones, soy Tony, del Instituto de Investigación del Cáncer. Estamos realizando la recaudación anual para apoyar nuestra investigación contra la enfermedad del cáncer, que asedia a hombres, mujeres y niños".

"Por favor, llámame Chuck", interrumpió.

Esto era buena señal, porque no me dio ninguna excusa ni intentó terminar la conversación diciendo que estaba ocupado; tomó la iniciativa de llevar la conversación a un plano más personal. Continué: "De acuerdo, Chuck, gracias. Estamos realizando esta recaudación entre empresas que han apoyado la causa del cáncer con anterioridad y estamos pidiendo pequeñas donaciones de entre 50 y 150 euros. Lo mejor es que todos los colaboradores pasan automáticamente a participar en una rifa con dos estupendos premios: dos entradas para ver a los Mets en Nueva York y una cena gratis para dos en un restaurante a elegir entre tres opciones. Hemos preparado cinco premios como éste".

"Vaya, un partido de los Mets, ¿eh?".

"Bueno, a lo mejor no te gustan los Mets, pero aun así los restaurantes son muy buenos".

"No, no, si me encantan los Mets, por eso lo decía".

"Bueno, piensa en esto: no sólo colaborarás con nuestra gran investigación, puedes conseguir entradas para un estupendo partido y una cena en Morton's, Basil's o Domingoes".

"¡Domingoes! ¡En serio! Me encanta ese sitio".

"Vaya, genial. Precisamente fui el otro día por primera vez y tomé su pollo Portabella. Estaba buenísimo". Ése era el tercero de sus platos favoritos.

"Pues si crees que ese plato es bueno, tienes que probar la pasta al Fra Diablo. Es el mejor plato que tienen. Yo lo pido siempre".

"Tenía pensado ir este fin de semana, así que lo probaré. Gracias por el consejo. Mira, ya sé que se está haciendo tarde. Ni siquiera te estoy pidiendo dinero ahora, nunca lo hago por teléfono. Lo que puedo hacer es mandarte un PDF; puedes echarle un vistazo y si estás interesado puedes enviarnos un cheque junto con el formulario".

"Perfecto, mándamelo".

"De acuerdo, sólo un par de preguntas. ¿Cuál es tu correo electrónico?".

"`chuck.jones@company.com`".

"Si puedes, abre tu Adobe Reader, haz clic en el menú Ayuda y después en Acerca de Adobe Reader y dime la versión del programa, por favor".

"Un segundo; es la 8.04".

"Estupendo; no quisiera enviarte una versión que no puedas leer. Un momento, te voy enviar el documento mientras hablamos. De acuerdo, ya está enviado".

"Perfecto, gracias. Espero ganar, porque me encanta ese sitio".

"Lógico, la comida es buenísima. Antes de despedirnos, ¿te importaría comprobar si has recibido el correo electrónico y si funciona bien?".

"Sí, claro. Me voy a desconectar en cinco minutos pero puedo comprobarlo. Sí, aquí está". Cuando escuché el sonido del doble clic, comprobé en BackTrack cómo Meterpreter (véase el capítulo 7), el recopilador malicioso de contenido, reaccionaba. Contuve el aliento (esta parte siempre es emocionante) y, ¡bam!, apareció la conexión. Los scripts del Meterpreter cambiaron la propiedad a algo así como `Explorer.exe`.

Entonces Chuck dijo: "Humm, la pantalla se queda totalmente en blanco. Y no reacciona".

"¿En serio? Qué raro. Deja que lo compruebe". Lo que estaba comprobando en realidad era si tenía acceso a su disco y la posibilidad de cargar una conexión inversa que se reiniciara en caso de que apagara el ordenador. Dije: "Lo siento, no sé qué ha pasado. ¿Puedes darme un minuto o te tienes que marchar?".

"Bueno, tengo que ir a dejar la taza de café en la cocina, así que vuelvo en unos minutos".

"Perfecto, gracias". Esos minutos era todo lo que necesitaba para asegurarme de que tenía acceso ilimitado e inverso a su ordenador.

"Ya estoy de vuelta".

"Verás, Chuck, estoy avergonzado pero realmente no sé lo que ha pasado. No quiero retenerte, así que si quieres vete a casa y te mando otro correo con un nuevo PDF. Si te parece, el lunes hablamos".

"De acuerdo. Que pases un buen fin de semana".

"Tú también, Chuck".

Nos despedimos y, para mi sorpresa y alegría, su ordenador permaneció activo. Efectivamente, guardaba la información en una unidad de disco a la que sólo él tenía acceso, pero en documentos Word. Descargué rápidamente esos documentos y en unas horas tuve acceso a los servidores e imprimí todos los procesos internos que el director intentaba proteger.

En efecto, hablé con él el lunes, pero no como Tony sino como su consultor de seguridad con copias impresas de sus "secretos", sus contraseñas y grabaciones de las conversaciones telefónicas que mantuvimos con él y con sus empleados.

En esta primera reunión siempre hay que contar con el asombro inicial del cliente y sus argumentos de que empleamos tácticas injustas y vulnerabilidades personales para lograr acceder. Cuando explicamos que los chicos malos emplearían exactamente las mismas tácticas, la mirada de enfado se transforma en una mirada de miedo y ese miedo se convierte en comprensión.

Aplicación del ámbito conceptual de la ingeniería social en el ataque al director general

Al igual que en los ejemplos previos, resulta beneficioso comparar el caso con el ámbito conceptual de la ingeniería social y comprobar lo que estuvo bien y los puntos que se podrían mejorar.

Como siempre, la recopilación de información es la base sobre la que se sustenta toda la acción y esta historia en particular lo demuestra. La recopilación de información desde distintas fuentes (la Web, Maltego, el teléfono, etc.) es lo que hizo de este ataque un éxito. La falta de información habría conducido a un fracaso estrepitoso.

La información completa y adecuada marca la diferencia, incluso datos que nunca hubiera necesitado, como su parroquia y los nombres de sus padres y sus hijos. Estos datos podrían haber sido útiles, pero lo que acabó teniendo un valor incalculable fue la información que encontré sobre el correo electrónico y los archivos en los servidores utilizando Maltego. Ésa fue mi vía de entrada a la empresa.

También es importante mantener la información catalogada en BasKet o Dradis, tal como se explica en el capítulo 2; en caso contrario, sólo tendría un documento de texto con información desordenada que no podría utilizar. Organizar la información es tan importante como recopilarla y utilizarla.

Pensar como los chicos malos (esto es, buscar las formas de explotar las debilidades y los deseos del objetivo) no es una parte muy importante del trabajo, pero si un auditor profesional quiere proteger a sus clientes, debe mostrarles lo vulnerables que son.

Cuanta más información recopile, más sencillo le resultará encontrar debilidades. Empezará a encontrar caminos hacia el éxito.

Desarrollar pretextos realistas y temas que tengan el máximo efecto sobre el objetivo también contribuye al éxito del ataque. Debe desarrollar preguntas poderosas y utilizar palabras clave que atraigan al objetivo. Al reunir toda esta información, fui capaz de plantear buenas preguntas y un encuadre que incluía palabras clave y palabras con poder neurolingüístico, que utilicé a continuación en tácticas de persuasión que sabía que funcionarían.

Tuve que cambiar mi pretexto, desde llamar a proveedores de la empresa a llamar a empleados en busca de información. Tuve que planear cada pretexto, meterme en el papel y seguirlo con eficacia. Esto, por supuesto, conllevó mucha preparación para que cada pretexto fuera convincente, se desarrollara con fluidez y tuviera sentido.

La práctica lleva a la perfección. Antes de lanzar el ataque, mi socio y yo practicamos mucho. Tuve que asegurarme de que los archivos PDF funcionaran y que la opción de ataque fuera razonable. También tuve que reunir los conocimientos suficientes para resultar creíble para todos los objetivos con los que hablara.

No debe subestimarse la importancia de la práctica. Gracias a ella pude comprender qué tácticas funcionarían y cuáles no y también tuve la seguridad de que podría seguir con el plan establecido sin preocuparme de la dirección que tomaran los acontecimientos.

Analizando el ataque en retrospectiva, he descubierto un par de detalles que podrían mejorarse para que el ataque fuera más efectivo. Por un lado, siempre es un riesgo depender exclusivamente de un PDF malicioso; debería haber creado un pequeño sitio Web que imitara la Web real del instituto de investigación contra el cáncer y haber cargado ahí el PDF. Tanto la Web como el PDF podrían haber contenido código malicioso. Esto habría duplicado mis opciones de tener éxito, además de haberme dado cobertura en caso de que alguna de las vías hubiera fallado.

Otro riesgo importante que tomé fue que el director dejara encendido el ordenador cuando se fue de la oficina. Si no lo hubiera hecho, tendría que haber esperado hasta el lunes para intentar acceder. Para mantenerlo en el ordenador debería haber preparado un PDF "real" con información que podría haber mandado después de que el PDF malicioso explotara su ordenador. De esta forma, habría mantenido al director en su ordenador el tiempo suficiente para aprovechar bien la explotación.

Esta auditoría nos llevó una semana de trabajo entre la investigación, la recopilación y organización de la información, la práctica y el lanzamiento del ataque. En una semana los secretos más importantes de esta empresa podrían haber estado en las manos de su competencia o del mejor postor. Repase la historia e intente comprender los métodos sutiles empleados y la forma en que fluyeron las conversaciones. Es difícil expresar por escrito la modulación de la voz, los tonos empleados y el ritmo de la conversación, pero intente imaginarse a usted mismo en esta conversación y piense cómo la resolvería.

Estudio de caso de Hadnagy 2: el escándalo del parque temático

Este caso me resultó muy interesante porque implicó algunas acciones a realizar en persona. Utilicé muchas de las habilidades de la ingeniería social mencionadas a lo largo del libro y las puse a prueba durante este caso.

También fue interesante por la naturaleza del negocio y el potencial para una estafa exitosa. El atacante podría haber tenido acceso a miles de números de tarjetas de crédito.

El objetivo

El objetivo era un parque temático preocupado por que su sistema de expedición de billetes se pusiera en peligro. Los ordenadores donde se registraban los clientes contenían un vínculo a los servidores, información de clientes y registros financieros.

El parque quería comprobar si existía la posibilidad de que un atacante empleara métodos malintencionados para conseguir que un empleado realizara alguna acción que pusiera en peligro el sistema.

La meta no era meter en problemas a un empleado, sino más bien comprobar el daño que podría causar un ataque a uno de los ordenadores de registro de clientes. Además, la meta tampoco era comprometer los ordenadores mediante un pirateo informático sino a través de tácticas de ingeniería social pura.

Si podía darse la situación de peligro, ¿cuáles eran sus ramificaciones? ¿Qué datos podían descubrirse y qué servidores se pondrían en peligro? No querían profundizar en exceso, simplemente averiguar si funcionaría la primera fase de un ataque de ingeniería social.

Para saber si era posible un ataque exitoso, primero debía comprender los procesos del parque y sus métodos para registrar clientes y las cosas que los empleados hacían y no hacían con sus terminales o, aun más importante, lo que podían y no podían hacer.

La historia

Como hemos mencionado, la meta en este trabajo no era especialmente compleja; sólo debía averiguar si el empleado de la taquilla permitiría que un "cliente" le hiciera realizar una acción no permitida. Antes de pensar cuáles eran esas acciones, debía comprender el negocio.

Navegué por el sitio Web del parque y utilicé Maltego y Google para investigar artículos y otra información sobre la empresa. También hice un poco de investigación de campo. Fui al parque y pasé por el proceso de comprar un billete en la taquilla.

Durante el proceso entablé una inofensiva conversación con la cajera y pasé algún tiempo observando la distribución, los nodos informáticos y otros aspectos del área de la "oficina".

Analizando esta área es donde se empezaron a aclarar mis ideas. Durante la conversación, le dije a la taquillera que yo era de una ciudad muy pequeña con un nombre muy largo. Cuando me preguntó el nombre y se lo dije, contestó algo muy normal:

"¿Dónde diablos está eso?".

"¿Tienes acceso a Internet desde aquí?".

"Sí".

"Pues te va a encantar. Entra en `maps.google.com` y escribe el código postal 11111 y activa la vista por satélite. Verás lo pequeña que es la ciudad".

"Oh, Dios mío; es minúscula; creo que no había oído hablar de este sitio en mi vida".

En este corto periodo de tiempo había averiguado lo siguiente:

- La distribución del espacio donde trabajaba un cajero.
- Cómo registraban a cada cliente.
- Que los ordenadores tenían acceso completo a Internet.

Volví a navegar por el sitio Web del parque con una nueva aclaración sobre sus procesos. Necesitaba encontrar una forma de acceder a su sistema informático. Mi pretexto era razonable: era un padre que llevaba a su familia al parque a pasar el día.

La historia era que no habíamos planeado la visita con antelación, pero en el hotel habíamos entrado en Internet para buscar cosas que hacer en la ciudad y encontramos un buen descuento para el parque. Bajamos al vestíbulo del hotel e intentamos comprar unos billetes pero el precio era bastante más alto que el que habíamos encontrado en Internet.

Comprobamos la oferta y nos dimos cuenta de que era una oferta exclusiva para Internet. Compramos los billetes y después nos dimos cuenta de que era necesario imprimir los billetes para poder escanearlos en la taquilla. Intenté imprimirlos en el hotel pero la impresora no funcionaba. Ya había pagado y estaba algo inquieto por temor a perder los billetes, por lo que los guardé en formato PDF y me los envíe a mí mismo por correo electrónico. Parece una historia razonable, ¿verdad?

Sólo faltaba un detalle para completar mi malvado plan. Tenía que hacer una llamada de teléfono:

"Hola, ¿la oficina del parque temático?".

"Sí; ¿qué puedo hacer por usted?".

Tenía que hablar con alguien de la oficina central y hacer mi pregunta y asegurarme de que obtenía la respuesta adecuada. Después de pedir que me pasaran con el departamento de compras, me pasaron con la persona adecuada. Dije: "Hola,

soy Paul de SecuriSoft. Estamos entregando versiones de prueba gratuitas de un nuevo software para leer e imprimir archivos PDF. Me gustaría enviarle la URL para la descarga gratuita, ¿le parece bien?".

"Bueno, no estoy seguro de que nos interese, pero puede mandarme la información si quiere".

"De acuerdo, perfecto. ¿Me puede decir qué versión de Adobe están utilizando actualmente?".

"Creo que trabajamos con la 8".

"Muy bien; hoy mismo le envío la información".

Una vez que supe la versión que utilizaban, lo único que tenía que hacer era crear un PDF malicioso con una consola inversa (que me daría acceso a su ordenador una vez que abriera el PDF), ponerle un nombre como `Recibo.pdf` y después enviármelo a mí mismo.

Al día siguiente, involucré a mi familia en una acción de ingeniería social. Mientras se mantenían esperando cerca de mí, me acerqué a la mujer de la taquilla y entablé una conversación amistosa.

"Hola, ¿qué tal estás... Tina?", dije, leyendo la placa con su nombre.

"Muy bien, ¿en qué puedo ayudarle?", dijo, con la típica sonrisa de cara al cliente.

"Verás, hemos decidido hacer una escapada de fin de semana y estoy hospedado con mi familia en el hotel Milton", dije, señalando hacia mi querida familia a unos metros de distancia. "Mi hija vio un anuncio de su parque y nos ha pedido que viniéramos y hemos accedido. Hemos encontrado una buena oferta en la Web...".

"Ah, sí, nuestra oferta exclusiva en Internet, está siendo todo un éxito. ¿Me da sus billetes, por favor?".

"Sí, verás, precisamente por eso necesito tu ayuda, para que no me den el premio al peor padre del año". Mi risa nerviosa fue correspondida por su sonrisa. Le expliqué la situación: "Tina, mi mujer y yo vimos la oferta y decidimos ahorrar un 15 por 100 y compramos los billetes a través del ordenador del hotel. El problema es que después de pagarlos no pudimos imprimirlos porque la impresora del hotel está estropeada. Lo que he hecho ha sido guardarlos en formato PDF y enviármelos a mi correo electrónico. Ya sé que le estoy pidiendo algo un poco extraño, pero ¿podría entrar en mi cuenta de correo electrónico e imprimir los billetes?".

La cuenta de la que hablaba era una cuenta genérica con los típicos mensajes con títulos como "Fotos de los niños" o "Aniversario de papá y mamá" y cosas por el estilo.

Resultó evidente que mi propuesta le generó muchas dudas y no estaba seguro de si su silencio me beneficiaba o si lo mejor era ayudarla a tomar una decisión. Dije: "Ya sé que es una petición extraña, pero mi hija se muere por

entrar en el parque y me sentaría fatal tener que decirle que no". Volví a señalar hacia mi hija, que estaba haciendo un buen trabajo resultando muy agradable pero impaciente.

"Está bien, ¿cómo lo hago?".

"Entra en `gmail.com` con el nombre de usuario `Paul12324@gmail.com` y contraseña S-E-L-I-S-T-A" (ya sé que esta contraseña es terrible, pero una advertencia de última hora nunca está de más. Pasó desapercibida).

Momentos después, Tina estaba abriendo mi PDF y obteniendo una pantalla en blanco.

"No me lo puedo creer. ¿Los he guardado mal? Vaya, ahora sí que me he ganado el premio al peor padre del mundo".

"¿Sabe qué? ¿Qué le parece si paga sólo los billetes de adulto y dejamos que su hija entre gratis?".

"Vaya, muchas gracias". Pagué los 50 euros con una sonrisa, le di las gracias por ayudarme y le pedí que cerrara mi correo electrónico. El resultado cuando nos separamos era una hija feliz y el parque temático en peligro.

Un poco más tarde, mi socio me mandó un mensaje diciéndome que había conseguido "acceder" y que estaba "reuniendo" información para el informe. Después de disfrutar de unas cuantas horas de relajación, nos fuimos del parque y volví al trabajo para organizar el informe para la reunión del lunes por la mañana.

Aplicación del ámbito conceptual de la ingeniería social en el ataque del parque temático

Como demuestra este caso, la recopilación de información no siempre se basa primordialmente en Internet; también puede realizarse en persona. La información más valiosa de esta auditoría se obtuvo mediante una visita en persona. Los componentes más importantes de la fase de recopilación de información fueron averiguar los sistemas informáticos que se estaban utilizando, tantear al objetivo para comprobar cómo reaccionaría a cierto tipo de preguntas y descubrir cómo funcionaba el sistema de expedición de billetes.

La conclusión en este ataque concreto es que un buen pretexto es más que una historia convincente; es más que un disfraz elaborado y un acento falso. Un buen pretexto es algo que se puede "vivir" sin mucho esfuerzo.

En este escenario fui capaz de hablar y actuar como un padre porque lo soy. Mi preocupación por ser un buen padre era real, no fingida y, por tanto, el objetivo la percibió como real. Esto hace que todo lo que se dijo resultara mucho más creíble.

Por supuesto, tener a una niña encantadora observando anhelante en la distancia ayuda mucho, como también lo hizo la historia de la impresora del hotel estropeada. El capítulo 2 trata estos temas, pero en ocasiones da la sensación de que el pretexto o la ingeniería social en general consisten simplemente en mentir bien. No creo que esto sea así.

Desde el punto de vista profesional, el pretexto implica crear una realidad que manipule las emociones y acciones del objetivo para que tome el camino que el atacante quiere que tome. La gente no suele sentirse motivada por una simple mentira. Es necesario "convertirse" en el personaje del pretexto; por eso, es buena idea emplear pretextos que le resulten fáciles de desarrollar por sus circunstancias personales.

El pretexto del "software gratuito para PDF" tenía un amplio margen de error. El pretexto era sólido, pero un rechazo habría supuesto un retraso de un par de días para poder lanzar el siguiente ataque. También fue un "golpe de suerte" que toda la empresa utilizara la misma versión de Adobe y que la taquillera que elegí no hubiera actualizado su Adobe a la nueva versión, lo que habría anulado mi intento de explotación. No suelo contar con la pereza inherente a la naturaleza humana, pero en este caso funcionó. En ocasiones, la mejor estrategia consiste en seguir hacia delante como si aquello que está pidiendo fuera trato hecho. Esa actitud genera un sentimiento de confianza y provoca que el objetivo crea que lo que está diciendo es legítimo.

Utilizar palabras o frases como "necesito tu ayuda..." es un arma poderosa, como se explica en el capítulo 5. A los seres humanos por naturaleza les gusta ayudar a los demás, sobre todo cuando se les pide que lo hagan.

En ese caso, hasta completos desconocidos harán lo posible por "echar una mano" incluso, como en éste, abriendo un archivo desconocido desde la cuenta de correo de otra persona. La excusa de ayudar a un "pobre padre" a conseguir llevar a su hija al parque puso en peligro todo el sistema.

Una vez comprometido, el software que almacena toda la información de las tarjetas de crédito de los clientes estaba abierto al atacante. La habilidad para extraer esa información sin apenas esfuerzo podría haber supuesto una pérdida tremenda para el parque, una lluvia de demandas y una situación muy embarazosa.

Estudio de caso de alto secreto 1: misión no imposible

De vez en cuando, mi socio o yo nos vemos envueltos o escuchamos alguna historia que nos encantaría que acabara convertida en una película, pero por razones de seguridad no estamos autorizados a escribir ni hablar de ella. Por este motivo no puedo mencionar a las personas implicadas en la historia que nos contó un ingeniero social llamado "Tim".

La meta de Tim era infiltrarse en un servidor que albergaba información que podía ser devastadora si caía en las manos equivocadas. La empresa de altos vuelos implicada tenía mucho que proteger. Cuando contrataron a Tim para obtener esta información corporativa, él sabía que tendría que llegar al límite; este trabajo pondría a prueba sus habilidades como ingeniero social.

El objetivo

El objetivo era una corporación de alto nivel que poseía ciertos secretos corporativos que bajo ningún concepto debían llegar a las manos de la competencia. Estos secretos se guardaban en servidores a los que no se podía acceder desde el exterior, sólo desde la red interna. Tim fue contratado para ayudar a la empresa a poner a prueba su sistema de seguridad contra "personas deshonestas" que pudieran ser capaces de infiltrarse y llevarse la valiosa información. Tim se reunió con una persona de la empresa en una localización externa, donde firmaron el contrato que habían desarrollado por teléfono y correo electrónico.

La historia

Tim se enfrentaba a un gran reto. El primer paso, como en cualquier acción de ingeniería social, era la recopilación de información. Al no saber qué información utilizaría y cuál descartaría, Tim fue a por todas, reuniendo información como la distribución de plan de correo electrónico, solicitudes de presupuesto, todos los nombres de empleados que pudo conseguir, además de las redes sociales a las que pertenecían, los artículos que habían publicado, clubes a los que pertenecían y los proveedores de servicios que utilizaban.

Quería buscar en los contenedores, pero cuando inspeccionó el área se percató de que estaba muy protegida por los guardias de seguridad. Además, muchos contenedores estaban encajados en zonas tapiadas, por lo que no podía ver el logo de la empresa que ofrecía el servicio. Cuando averiguó cuál era el departamento que se encargaba de tratar con la empresa de recogida de residuos, decidió realizar una llamada muy bien planeada:

"Hola, soy Paul de la empresa X de recogida de residuos. Estamos ofreciendo un nuevo servicio en la zona y estamos trabajando con muchas de las empresas más importantes. Yo formo parte del departamento de ventas y estoy encargado de esta región. ¿Podría enviarle un presupuesto de nuestros servicios?".

"Bueno, estamos satisfechos con el servicio que recibimos actualmente, pero puede mandarnos el presupuesto si lo desea".

"Perfecto; ¿puedo hacerle unas preguntas rápidas?".

"Claro".

"¿Cuántos contenedores tienen?", preguntó Tim. Después de preguntar si tenían contenedores separados para papel y residuos tecnológicos como llaves USB y discos duros, dio los últimos retoques.

"¿Cuál es el día normal de recogida?".

"Tenemos dos recogidas semanales; la serie 1 los miércoles y la 2 los jueves".

"Gracias. Voy a preparar su presupuesto, lo tendré listo mañana por la tarde. ¿A qué dirección de correo electrónico lo puedo enviar?".

"Mándemelo a mí, a `christie.smith@company.com`".

A continuación, entabló un poco de cháchara amistosa y antes de darse cuenta estaban compartiendo risas e intercambiando bromas.

"Muchas gracias. Por cierto, antes de colgar, ¿puedo preguntarte con qué compañía estáis trabajando? Me gustaría preparar un presupuesto comparativo".

"Bueno, verás...". Dudó por un momento, pero finalmente dijo: "Claro, trabajamos con Wasters Management".

"Muchas gracias, Christie, me aseguraré de que el presupuesto sea de tu interés. Hablamos pronto".

Con esta información, Tim entró en el sitio Web de la empresa de recogida de residuos y guardó una copia de su logo en un archivo JPG. Después acudió a una imprenta de camisetas *on-line* y en 72 horas tenía una camisa con el logo bordado. Sabiendo que recogían la basura los miércoles y los jueves, planeó ir el martes por la noche.

Entonces hizo otra llamada, esta vez al servicio de seguridad:

"Hola, soy John de Wasters Management, su empresa de recogida de residuos. Nos ha llamado Christie Smith para decirnos que tienen un contenedor estropeado. Como la recogida es el miércoles, me gustaría pasarme mañana por la noche para comprobarlo. Si la unidad está dañada haré que el camión traiga una nueva. ¿Le parece bien que vaya mañana por la noche?".

"Sí, claro, déjeme hacer una comprobación. Sí, mañana está Joe. Cuando llegue, pare en la garita de seguridad y le dará una chapa identificativa".

"Muchas gracias".

Al día siguiente, Tim se vistió con su camisa de la "empresa" y llevó una carpeta. El pretexto era genial porque conocía las fechas y los nombres de los empleados. Ahora, con el aspecto de un trabajador de la empresa, se acercó a la garita del guardia.

"Joe, soy John de Wasters, llamé ayer".

El guardia le interrumpió: "Sí, aquí tengo anotado su nombre". Le dio la chapa y un mapa para que supiera llegar a los contenedores. "¿Necesita que le acompañemos?".

"No, hago esto continuamente".

Tim entró y condujo hasta los contenedores.

Con este pretexto perfecto y la chapa identificativa, Tim tenía tiempo para hurgar en los contenedores. Sabía que la serie 2 eran los residuos no orgánicos, así que empezó por ahí.

En unos instantes, había cargado en su camioneta varios discos duros, llaves USB, algunos DVD y varias bolsas con papeles. Al cabo de una hora volvió, dio las gracias a los guardias de seguridad y les aseguró que todo estaba en orden. De vuelta en la oficina analizó la "basura" y se topó con un regalo que no podía haber imaginado ni en sus mejores sueños.

Muchas veces las empresas se deshacen de discos duros y hardware USB destruyéndolos completamente. Borran todos los datos y después lo envían a unidades especiales de eliminación de residuos. No obstante, de vez en cuando, algún empleado desconocedor del procedimiento simplemente tira a la basura una llave USB estropeada o un disco duro que no funciona bien. Lo que no saben es que existen muchos programas que pueden extraer datos incluso de hardware estropeado. Incluso si el disco ha sido formateado, en ocasiones se puede recuperar la información.

Una de las bolsas contenía lo que parecía material de oficina. Al vaciar la bolsa descubrió que había papeles que no habían pasado por el triturador. Se sentó a leerlos y vio que uno de ellos era un contrato de ciertos servicios tecnológicos anulado. El trabajo debía empezar en unos días, pero parecía que esa copia se había manchado de café y la habían descartado.

Esto suponía un gran hallazgo, pero había mucho más entre lo que rebuscar. Los DVD estaban en blanco o no se podían leer pero, sorprendentemente, pudo recuperar archivos de las llaves USB. A partir de estos documentos, descubrió el nombre y las líneas privadas del director de finanzas y de otros ejecutivos importantes.

El valor de lo que encontró era inmenso, pero me gustaría centrarme en lo que hizo a continuación. A la mañana siguiente, con el contrato de servicios tecnológicos en la mano y sabiendo el tipo de trabajo que se iba a realizar, llamó a la persona de contacto que aparecía en el contrato, a la hora del almuerzo, rezando para que esa persona hubiera salido a comer.

"Hola, ¿está Sebastian?".

"No, ha salido a comer. ¿Puedo ayudarle?".

"Soy Paul, de X Tech. Quería confirmar que nuestro equipo irá mañana por la tarde para empezar el proyecto".

"Sí, pero recuerde que no podemos sufrir ninguna interrupción del servicio, así que, por favor, no vengan antes de las cinco y media".

"Por supuesto. Hasta mañana".

Al día siguiente, Tim sabía que no podría ir con el resto del "equipo". Pero si calculaba bien los tiempos no sería descubierto por la empresa de servicios ni por el objetivo. Sentado en el aparcamiento, observó la llegada del equipo de la

empresa de servicios tecnológicos. Esperó media hora y después fue a la puerta de entrada donde explicó que había salido un momento para coger unos papeles del coche. Le dejaron entrar y entonces era el rey de la oficina.

Tenía que hacer un trabajo de reconocimiento y pensó que lo mejor sería abordar a la empresa de servicios como si fuera un empleado interno. Dio vueltas por las oficinas hasta que escuchó a alguien hablando y vio a un hombre vestido con una camisa que le identificaba como uno de los empleados de la empresa de servicios.

Sabiendo los nombres de varios superiores y el de la persona de contacto del contrato, inició la conversación: "Hola, soy Paul, trabajo para el señor Shiraz (el director de finanzas). ¿Alguien les ha explicado algo sobre el servidor prod23?". Tim conocía el nombre del servidor por su recopilación de información y sabía que ése era el servidor que tenía que atacar.

"Sí, sabemos que ese servidor es zona vedada. El director nos ha explicado el encriptado y que no debemos tocar ese servidor. No hay problema".

Tras unos minutos de conversación, Tim tenía información muy valiosa:

- El equipo contratado no tenía permitido tocar el servidor.
- El servidor tenía encriptación de disco completa.
- El técnico de la empresa había alardeado sobre el fichero de llaves que utilizaban y que estaba en una llave USB que sólo tenían los administradores.

Tim sabía que este último punto haría su tarea más complicada. Los administradores no estaban en ese momento, por lo que no podía entrar en el servidor por ahora. Además, había personal de seguridad en la zona donde estaba el servidor y no merecía la pena correr el riesgo. Sabía que los administradores accederían a ese servidor por lo que pensó que podía intentar esa vía.

Fue al despacho del primer administrador, pero estaba cerrado con llave. Comprobó el segundo despacho y después el tercero. El tercero no estaba cerrado con llave, así que entró.

Cerró las persianas y dejó las luces apagadas, para evitar ser descubierto. En su equipo contaba con una gran variedad de herramientas y vestuario. Una de las herramientas que siempre llevaba encima en este tipo de actuaciones era una llave USB con una distribución Linux de arranque como BackTrack. La instalación BackTrack incluye una versión precargada de Virtual Box, una máquina virtual de fuente abierta.

Cargó el ordenador del administrador en BackTrack utilizando un puerto USB. Después, conectó con sus propios servidores vía SSH, estableció un receptor y volvió a conectar con él empleando una consola inversa que había iniciado desde el ordenador del administrador. Luego, inició un rastreador de teclado

(para registrar todas las pulsaciones de teclas del ordenador) en BackTrack y preparó el archivo de registro para que se volcara en su ordenador a través de la conexión SSH.

Después, hizo algo verdaderamente pernicioso. Abrió Virtual Box y creó una máquina virtual de Windows, utilizando el disco duro local como medio físico desde el que iniciar y cargó la máquina virtual. Automáticamente cargó el perfil de usuario del administrador y el sistema operativo. En la pantalla de inicio de sesión cargó la máquina virtual para que estuviera en modo de pantalla completa, ocultó todas las barras e hizo que la tecla de acceso rápido para salir de Virtual Box fuera una combinación de teclas increíblemente larga. De esta forma evitaba que el usuario introdujera fortuitamente la combinación y descubriera que estaba siendo pirateado.

Todavía existía el riesgo de que fuera descubierto en cualquier momento utilizando este método de una llave USB cargada con una máquina virtual utilizando su propio disco duro pero, si funcionaba, conseguiría registrar cada pulsación de teclas del administrador y una conexión a su ordenador, dándole a Tim acceso a todo lo que hubiera en él. Incluso aunque la conexión estuviera en la máquina virtual, registraría todas las pulsaciones de teclado para después acceder al ordenador de la víctima empleando el nombre de usuario y la contraseña capturados.

Tim hizo algunas otras cosas mientras estuvo en la oficina, como establecer una conexión en otro ordenador, que le daría acceso remoto a la red. También estableció un receptor remoto, del tipo que utiliza una tarjeta SIM de telefonía móvil. Podía llamar al número desde cualquier parte del planeta y escuchar las conversaciones que tuvieran lugar en seis metros a la redonda.

Unas horas después, Tim se marchó de la sede de la empresa y volvió a su oficina. Estaba expectante por ver si todos estos preparativos habían funcionado, pero aún tenía algunas ideas que podía probar.

A primera hora de la mañana siguiente, comprobó que sus conexiones remotas aún funcionaban y marcó su receptor para escuchar el rumor de la gente llegando a la oficina. La expectación fue creciendo mientras esperaba los primeros registros para ver si capturaba el nombre y contraseña del administrador.

Una hora después, Tim observó los primeros registros. Sabía que no debía hacer nada que pusiera en peligro su conexión, por lo que se mantuvo a la espera. Sobre las doce y cuarto se detuvieron los registros, por lo que supuso que el administrador se había ido a almorzar. Rápidamente, comprobó su consola inversa y comenzó a crear un túnel desde el ordenador del administrador al servidor y de vuelta a su ordenador utilizando la contraseña que obtuvo del administrador del servidor.

Una vez que el túnel estuvo conectado, empezó una carrera frenética para copiar todo lo que pudiera antes de la una de la tarde. En ese momento no detectó ningún registro, por lo que conectó con el receptor y escuchó a alguien preguntando: "¿Sabes cuánto tiempo va a durar la reunión?".

Suponiendo que el administrador iba a estar en una reunión hizo un nuevo intento con una transferencia más larga. Al cabo de media hora detectó cierta actividad, por lo que detuvo la recopilación de datos y decidió esperar hasta más tarde. No quería alertar al administrador ralentizando su conexión debido a la transferencia. Comenzó a filtrar lo que había extraído del servidor, sabiendo que había dado en el clavo.

Su trabajo no había terminado aún. Esa tarde llevó a cabo una nueva transferencia masiva, extrayendo todo lo que pudo y después volviendo a la oficina de la empresa, utilizando un pretexto de nuevo para entrar. Una vez dentro, se dirigió al despacho del administrador, que esta vez estaba cerrada con pestillo. Empleó un cuchillo *shove* (véase el capítulo 7) para entrar.

Dentro del despacho apagó la máquina virtual. Reinició el ordenador después de extraer la llave USB y después se marchó dejando el despacho tal como se lo había encontrado. Recogió su receptor y se aseguró de no dejar rastro.

Salió del edificio y se dirigió a su oficina para ordenar sus hallazgos. Por supuesto, en la reunión posterior con la empresa, se presentó con una pila de documentos impresos y un disco duro repleto con todo lo que había conseguido copiar. Esto fue suficiente para que todas las personas de la sala se quedaran con la boca abierta.

Aplicación del ámbito conceptual de la ingeniería social en el caso de alto secreto 1

Esta historia ofrece muchas lecciones. Es un gran ejemplo de ingeniería social perfecta. Se puede resumir en práctica, preparación y, por supuesto, recopilación de información. Podemos suponer que practicó previamente todas las habilidades que puso en juego, desde utilizar un cuchillo *shove*, crear un túnel o el empleo de pretextos y la recopilación de información.

Nunca me cansaré de repetir la importancia de la recopilación de información. Sé que lo he dicho miles de veces, pero toda esta actuación habría fracasado si Tim no hubiera dispuesto de la información adecuada.

El éxito fue el fruto de la preparación mediante llamadas telefónicas, visitas en persona y contar con el hardware adecuado. Analizando este ataque puede ver en juego varios de los principios fundamentales de la ingeniería social.

Tim fue un maestro de la recopilación de información, empleando recursos Web para extraer oro y demostró ser un experto en la manipulación para obtener información al teléfono, así como una habilidad increíble para la persuasión en persona. Estas técnicas le permitieron reunir una información que probablemente habría pasado desapercibida a un hacker inexperto.

La recopilación de información le dio a Tim la base para desarrollar sus pretextos y las preguntas a realizar. La incursión en los contenedores se planeó con precisión milimétrica. ¿Hubiera tenido alguna opción de que le dejaran pasar sin la camisa con el logo y una cita? Posiblemente. Sin embargo, ¿no resultó mucho más convincente en el modo en que lo hizo? No despertó la más mínima sospecha y permitió a cada persona con la que interactuó que se olvidara de él al instante sin preocuparse por nada. Ése es el pretexto perfecto, cuando la persona con la que se interactúa no llega a sospechar nada. Tim lo consiguió y gracias a eso tuvo la libertad de moverse como si perteneciera a aquel lugar.

La mejor parte de la historia es lo que sucedió cuando entró en el edificio. Había un gran margen de error y podía haber sido descubierto varias veces. Por supuesto que podría haber extraído la información del servidor e irse y seguramente nadie le hubiera detenido, pero al hacerlo como lo hizo la empresa nunca se habría dado cuenta de cómo habían sido revelados sus secretos ni que estaban en peligro.

Tim asumió un gran riesgo cuando dejó el ordenador del administrador ejecutando una máquina virtual. Esa maniobra en particular podría haber fracasado de muchas maneras. Si alguien hubiera reiniciado el ordenador o si se hubiera colapsado o si por error el administrador hubiera presionado esa extraña combinación de teclas, habría acabado con el ataque y la empresa se habría percatado de la situación.

Yo habría seguido un camino diferente y menos arriesgado. Habría creado un túnel inverso desde su ordenador a mis servidores utilizando un EXE personalizado que no pudiera ser detectado por el software antivirus o en los scripts de arranque del ordenador, algo con menos probabilidades de fracasar, pero el método de Tim tuvo el don de ser un ataque de ingeniería social muy atractivo.

Probablemente, se pueden extraer varias lecciones de este ataque, pero sobre todo se aplica el viejo dicho hacker "no te fíes de nadie". Si alguien llama diciendo que Christine ha autorizado una inspección de los contenedores y no ha oído hablar de ello con anterioridad, llámela y pregunte. Apague los ordenadores por la noche y, sobre todo, no permita que los ordenadores se puedan iniciar desde una llave USB sin una contraseña.

Por supuesto, estas medidas extraordinarias conllevan más tiempo. El hecho de que merezcan la pena dependerá de la importancia de la información que guarden esos ordenadores. En este caso, esa información tenía la capacidad de arruinar a la empresa, por lo que la protección debería haber sido extrema. Aunque la empresa tomaba varias medidas de seguridad excelentes, como utilizar encriptación completa de disco, cámaras, cerraduras biométricas, etc. alrededor de la zona de servidores, todo esto no protegía los ordenadores que contenía la información más importante y esto es lo que puso a la empresa en peligro.

Estudio de caso de alto secreto 2: ataque de ingeniería social a un hacker

Pensar rápido y desde puntos de vista originales es práctica habitual del ingeniero social, por lo que es extraño encontrarse en una situación que desafíe a un profesional hasta el punto de dejarlo perplejo. ¿Qué sucede cuando se recurre a un probador de seguridad para que lleve a cabo una acción profesional sin previo aviso?

La siguiente historia muestra exactamente lo que ocurre cuando se produce esa situación. Es un buen ejemplo de la utilidad de tener practicadas de antemano algunas habilidades de ingeniería social por si fuera necesario aplicarlas en un imprevisto.

El objetivo

"John" fue avisado para que realizara una prueba de seguridad de red estándar para uno de sus clientes más importantes. Era una prueba que no requería habilidades de ingeniería social ni trabajo de campo. Aun así, disfrutó poniendo a prueba las vulnerabilidades de las redes de su cliente.

En esta prueba no estaba sucediendo nada especialmente emocionante. Llevaba a cabo su rutina, barriendo y registrando datos y probando ciertos puertos y servicios que creía que le podrían proporcionar una vía de entrada.

Casi al final de la jornada hizo un barrido utilizando Metasploit que puso al descubierto un servidor de VNC abierto, un servidor que permite controlar otras máquinas de la red. Éste fue un buen hallazgo, porque la red estaba cerrada y una vía de entrada tan sencilla era bienvenida.

John estaba documentando el hallazgo con la sesión de la VNC abierta, cuando de pronto el cursor del ratón empezó a moverse por la pantalla. Esto era una señal de alarma importante, porque con este cliente y a esa hora del día no podía haber ningún usuario conectado y utilizando el sistema por motivos legítimos.

¿Qué podría estar pasando? Observó que, en lugar de actuar como un administrador o un usuario normal, la persona se comportaba como si no conociera bien el sistema. John empezó a sospechar que había un intruso en la red. No quería espantarlo, sino averiguar si se trataba de un administrador o un hacker que había conseguido entrar en el sistema.

En un momento, el objetivo pasó de ser la empresa que le había contratado a ser un pícaro hacker que había penetrado en la organización.

La historia

John decidió que tenía que llevar a cabo un trabajo de ingeniería social sobre este hacker para sonsacarle toda la información que pudiera para ayudar a proteger a su cliente. En realidad, no tenía tiempo para pensar en cada paso y planear la acción adecuadamente. Tampoco tenía tiempo para llevar a cabo la pertinente recopilación de información.

Asumiendo un gran riesgo, abrió el bloc de notas. Rápidamente desarrolló el pretexto de que era un "n00b", un hacker novato, alguien sin los conocimientos necesarios que había encontrado esta vía abierta y la estaba pirateando, igual que el otro tipo.

Consiguió guardar algunas capturas de pantalla de la conversación. Eche un vistazo y observe el trabajo que hizo el ingeniero social sobre el hacker, como muestra la figura 8.1. John es el que inicia la conversación y cada línea es uno de ellos alternativamente.

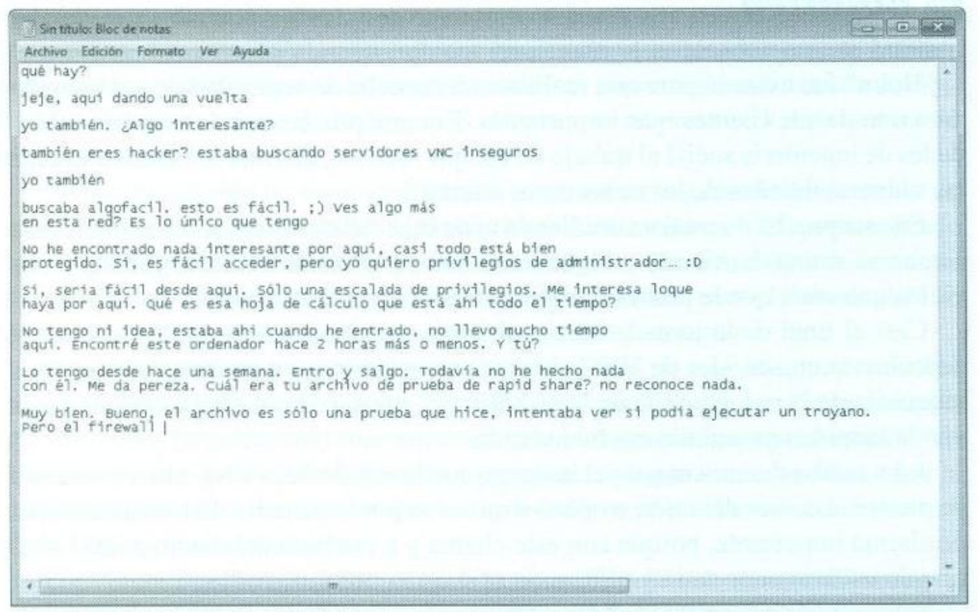


Figura 8.1. *Una captura de pantalla de la conversación.*

A continuación, tiene la transcripción al pie de la letra de la conversación que tuvo lugar. Es larga e incluye las erratas y la jerga que aparecen en el original, pero la transcripción muestra exactamente lo que sucedió en este ataque. John habla primero.

>> qué hay?
>> jeje, aquí dando una vuelta
>> yo también. ¿Algo interesante?
>> también eres hacker? estaba buscando servidores VNC inseguros
>> yo también
>> buscaba algofacil. esto es fácil. ;) Ves algo más en esta red? Es lo único que tengo
>> No he encontrado nada interesante por aquí, casi todo está bien protegido. Sí, es fácil acceder, pero yo quiero privilegios de administrador… :D
>> Sí, sería fácil desde aquí. Sólo una escalada de privilegios. Me interesa loque haya por aquí. Qué es esa hoja de cálculo que está ahí todo el tiempo?
>> No tengo ni idea, estaba ahí cuando he entrado, no llevo mucho tiempo aquí. Encontré este ordenador hace 2 horas más o menos. Y tú?
>> Lo tengo desde hace una semana. Entro y salgo. Todavía no he hecho nada con él. Me da pereza. Cuál era tu archivo de prueba de rapid share? no reconoce nada.
>> Muy bien. Bueno, el archivo es sólo una prueba que hice, intentaba ver si podía ejecutar un troyano. Pero el firewall no me ha dejado.
>> lol. Yo he tenido el mismo problema. Hice un shell de metasploit y no funcionó. Por eso sigo usando esto. Estás en EEUU? o fuera del país? conozco gente en Dinamarca.
>> De hecho soy de Noruega, jeje, tengo parientes en Dinamarca.
>> Entras en algún foro? a mí me gustaban algunos pero han desaparecido
>> Normalmente entro en algunos foros de programación, pero no mucho más. Llevas mucho tiempo pirateando? cuántos años tienes por cierto? Yo 22.
>> Llevo haciendo esto por diversión un año más o menos. Voy al colegio todavía. 16. Por hacer algo. Entras en evilzone?
>> De momento no. Yo también hago esto por diversión, para ver de lo que soy capaz, probar mis habilidades. Escribí el "Zinder VNC" yo mismo, por cierto, he encontrado varios servidores, pero este es el único un poco entretenido
>> Vaya. En qué lo escribiste? Puedo descargarlo? Tienes un controlador?
>> Está escrito en un lenguaje llamado PureBasic, pero todavía no está listo del todo, es para uso propio. A lo mejor puedo compartirlo de todas formas, puedo subir el código a algún sitio para que lo puedas compilar. Eso sí encuentras un compilador de PureBasic en algún sitio warez :P
>> Muy bien. puedes ponerlo en ese pastebin de irc. Nunca he hecho purebasic antes, sólo python y perl
>> Dejame ver, voy a buscar el sitio del pastebin y lo subo, dame unos minutos, estoy por aquí.
>> Ok gracias! tienes un controlador? soy jack_rooby
>> Controlador, para qué? No chateo en irc ni nada de eso, pero puedo darte un email donde puedes encontrarme.
>> Perfecto. Me refiero a un controlador para irc y boardz y eso. el correo también vale.
>> Sí, en el foro de programación compartí mi nombre completo, etc. A lo mejor no es buena idea. Mi correo es: intruder@hotmail.com
>> Mándame un mensaje o algo, a lo mejor puedo agregarte a msn.
>> Te mando una nota. Es bueno conocer a alguien que sepa programar este tipo de cosas por si me quedo atascado o encuentro algo bueno
>> Jeje, sí, podemos formar un equipo :P
>> Genial! avísame cuando tengas el pastebin
>> http://pastebin.ca/1273205
>> por cierto… esto está en la primera fase en realidad, la GUI no está terminada. pero se puede configurar con algunas variables.
>> Genial. Lo voy a probar a ver qué puedo hacer con él. Gracias por compartirlo, si consigo hacer algo interesante puedo enviártelo?

>> Sí, por favor. Si ejecutas ese programa unas horas encontrarás muchos servidores, incluso he intentado hacer código para detectar servidores desprotegidos y también alguno con un error que te deja registrarte sin contraseña. Esos servidores aparecen en el resultado (la "pestaña localizado") como "inseguro". Pero algunas veces da un error y dice que son inseguros algunos que no lo son, pero son pocos, sólo es para probarlos.

>> Vaya. He visto otros servidores vnc por aquí, pero todos piden contraseña. Tú herramienta deja que entremos?

>> Muy pocos tienen el error que te deja entrar, pero tienes que utilizar el cliente especial para ellos, aquí tienes más info:

>> http://intruderurl.co.uk/video/

>> Descarga el archivo zip

>> Olol, lo siento

>> lo siento. Ok, lo descargo y echo un vistazo. Genial. También has escrito la puerta trasera de rapad share? o has conseguido esto de otro sitio?

>> Intento escribir yo mismo la mayoría de mis herramientas, así aprendo. Lo he escrito yo, sí, pero no está terminado, sólo quería comprobar si podía ejecutar un servidor, pero todavía no hace nada, jeje.

>> Ya veo. Yo me he rendido, pero creo que voy a intentarlo otra vez.Me imagino que debe haber algo por ahí pero no tengo un botnet propio para usar, un tipo llamado Zoot54 intentó venderme uno, algunas personas lo respaldaban pero no me fiaba de él en absoluto. Y tampoco sé escribir mis propias herramientas aparte de un poco de perl y python, que no funcionan para la mayoría de hosts de Windows como este así que he estado probandoel metasploit pero me encuentro con el error del firewall. Tienes alguna idea para esto? Algo para solucionarlo? o simplemente pasar al siguiente?

>> Perl y python están bien para empezar, yo no los uso, pero cuando conoces más lenguajes puedes aprender más :P A lo mejor deberías probar PureBasic, es muy fácil. Jeje, un botnet estaría bien, estaba pensando en crear uno, pero es bastante difícil extenderlo, por lo menos en Vista. Pero no, no puedo dejar este servidor todavía, quiero seguir probando, tiene que haber una forma de conseguir más privilegios ;D

>> genial. Puedes estar con el servidor como he estado yo, sin saber qué hacer. dime lo que estás haciendo si no te importa para que pueda aprender un poco. Estaría bien. tienes myspace o facebook o algo? O sólo usas el correo?

>> Con el correo está bien por ahora, cuando confíe más en ti a lo mejor te agrego a facebook, no tengo myspace. Sí, te mantengo al tanto :)

>> Genial me parece bien. Tienes un shell o tienes esta misma gui? Es una multiconexión vnc?

>> Sí, uso ThightVNC o lo que sea y hago que no desconecte otros usuarios. No soy muy fan de los shell, la verdad, jeje :S

>> Jaja, he mirado la zona horaria y están en medio de EEUU así que es media noche para ellos.

>> Sí, yo he hecho lo mismo. Incluso he hecho una prueba de velocidad de la conexión de internet, jeje.Parece que tienen más velocidad de subidas que de bajadas, qué raro... Pero a lo mejor está bien para un ataque DoD.

>> DoS, quiero decir.

>> qué raro me pregunto qué tipo de línea será dice que es de co. tiene un nombre gracioso... Alguna vez consigues algún otro sistema por aquí? una vez vi un servidor warez pero fue hace mucho y ya no está.

>> No he encontrado más sistemas. Per me gustaría acceder a todos estos ordenadores que tienen en red... tienen muchos, parece una universidad. Jeje, hoy he impreso "hola mundo".

>> Jaja lo enviaste a una impresora o por pantalla? esta gente seguro que se pone nerviosa si ven que el ratón se empieza con esa extraña hoja de cálculo

>> Jaja, seguro que sí, pero esos idiotas ejecutan un servidor VNC sin contraseña?!

```
Lo he enviado a alguna de las impresoras, espero que lo vea alguien.
>> Jaja es verdad, apuesto... bueno no pueden ejecutarlo sin privilegios de
administrador no? Así que no puede haber sido un usuario, algún administrador ha
tenido que hacerlo o si no nuestras puertas traseras funcionarían y no lo hacen. O
crees que alguien ha cambiado la configuración?
>> Hmmm, bueno, creo que tienes razón, a lo mejor un administrador o un bromista...
>> Tú te dedicas a esto? He oído que se puede ganar dinero con esto, y creo que si
lo hago durante un tiempo y voy mejorando puedo conseguir un trabajo. Tú has hecho
eso?
>> He ganado dinero programando, pero nunca con temas de hacker o de seguridad. Pero
es buena idea, la gente paga para que pongan a prueba sus sistemas de seguridad y si
llegamos a ser buenos a lo mejor ganamos mucho dinero con esto.
>> Eso espero. Compré el libro del hacker ético y creo que tiene buenos programas.
No sé qué edad hay que tener para hacer la prueba, pero hacerla puede ser un buen
punto de partida para dedicarse a esto. También tiene buenas herramientas como el
metasploit. Deberías echarle un vistazo si no lo has hecho ya.
>> Sí, gracias, tengo que echarle un vistazo :) Pero estoy un poco cansado, jeje.
No puedo pasarme todo el día chateando en el bloc de notas, jejejeje. Nos vemos más
tarde, un placer conocerte, ha sido divertido.
>> Sí me asusté un poco cuando vi el rapid share en la pantalla. Un placer conocerte
te enviaré un correo para explicarte cómo funciona el programa. Está bien probarlo a
ver qué pasa. Cuídate y no dejes que te cojan los chicos malos!
>> Jeje, gracias, igualmente! :) Ha sido interesante, creo que voy a guardar esta
entrada del bloc de notas, dame un segundo, lol...
>> vale, lol, lo siento
>> adiós
>> adiós
```

Este chat muestra lo rápido que John tuvo que desarrollar su pretexto para convertirse en otra persona. Esto no es tarea fácil, ya que normalmente conlleva mucha preparación, pero para proteger a su cliente y averiguar quién era el intruso, tenía que representar el papel en el que le pusiera el hacker.

Finalmente, John consiguió obtener su foto, su correo electrónico y su información de contacto. Informó de este hacker a su cliente y se solucionó el problema para que no pudiera seguir entrando y saliendo de sus sistemas. Este caso de alto secreto demuestra cómo la utilización profesional de la ingeniería social puede ayudar a proteger a los clientes.

Aplicación del ámbito conceptual de la ingeniería social en el caso de alto secreto 2

Un punto interesante de esta historia es que en realidad la empresa no era el objetivo del hacker. Simplemente estaba barriendo Internet en busca de alguna "presa fácil" y eso es exactamente lo que encontró. Las máquinas abiertas con acceso completo son peligrosas y esta historia demuestra el gran daño que podría

haber ocurrido si el auditor de seguridad no hubiera estado allí en el momento preciso. Por supuesto, se puede aprender mucho sobre ingeniería social de esta historia. John no empezó este proyecto con la idea de emplear sus habilidades de ingeniería social. Era simplemente una mera prueba de seguridad. En ocasiones, es necesario emplear las habilidades sin haberlo podido planear previamente.

¿Cómo fue capaz John de hacerlo sin tener que irse a su casa a planear la acción? Seguramente, John utiliza estas habilidades a diario o, al menos, las ha practicado tanto que puede recurrir a ellas con gran facilidad.

La lección principal que se puede aprender de esta historia es que la práctica lleva a la perfección. John podía haberse enfrentado al hacker, haberle dicho que era un administrador, que le habían detectado y que iban a ir a por él. Se hubieran cruzado todo tipo de amenazas y podía haber empleado el miedo en su táctica.

Seguramente, el hacker habría desaparecido para volver más tarde a intentar formatear el sistema o hacer mucho más daño para ocultar su rastro. Sin embargo John, pensando muy rápido, fue capaz de recopilar información muy valiosa de su objetivo. Más tarde, John utilizó el correo electrónico y el nombre del objetivo y con la ayuda de Maltego se formó una idea muy clara de sus actividades.

Otro punto al que prestar atención en esta historia es la necesidad de ser fluido. A lo que me refiero es a aprender a seguir la corriente. Cuando John empezó a "recopilar información" del hacker, en realidad no sabía si esta persona era un hacker o un administrador. La primera línea de John, "¿qué hay?", podía haber sido respondida por el atacante de muchas maneras. Sin saber el tipo de respuesta que obtendría, John no tuvo tiempo para prepararse en realidad. Tuvo que utilizar la jerga y reaccionar del modo en que imaginaba que lo haría un hacker.

John fue incluso un paso más allá. Sabiendo que la mejor estrategia era permanecer sumiso, John indicó en el pretexto que era un "n00b" o hacker novato que no sabía demasiado y necesitaba que le enseñara un hacker real y experimentado. Alimentando el ego del hacker, John consiguió que revelara muchas cosas, incluido su nombre y una fotografía.

Por qué son importantes los estudios de casos

Estos estudios de casos prácticos son sólo algunas de las historias que ocurren ahí fuera y no son ni mucho menos las más asombrosas. Todos los días los gobiernos, plantas nucleares, corporaciones multimillonarias, redes de distribución e incluso países enteros son víctimas de ataques de ingeniería social maliciosos, sin incluir estafas personales, robos de identidad y hurtos que ocurre a cada momento.

Por muy triste que resulte leer estas historias, una de las mejores maneras de aprender es revisando los casos prácticos. Expertos de todos los campos utilizan esta metodología. Los médicos y los psicólogos revisan incontables horas de cintas y entrevistas para estudiar las microexpresiones que utiliza la gente cuando experimenta ciertas emociones.

Los expertos en persuasión revisan, analizan y estudian casos de persuasión positiva y negativa. Hacerlo les ayuda a llegar a las áreas más escondidas que afectan a las personas y a ver cómo pueden utilizarse para aprender y proteger a sus clientes. Las fuerzas del orden revisan casos prácticos como parte de su actividad diaria para aprender lo que motiva a los criminales. En ese sentido, los investigadores analizan y diseccionan todos los aspectos de los criminales, incluyendo lo que comen, cómo interactúan con los demás, lo que piensan y lo que les hace reaccionar. Toda esta información les ayuda a comprender realmente la mente del criminal.

Estos mismos métodos son los que utilizan los perfiladores para detectar a los "chicos malos". Del mismo modo, los ingenieros sociales maliciosos aprenden mucho estudiando no sólo sus propios casos prácticos sino otros de su mismo campo y las historias que encuentran en las noticias. Revisando casos prácticos el ingeniero social puede empezar a ver las debilidades de la psique humana y el porqué de que las tácticas de ingeniería social funcionen con tanta facilidad. Éste es el motivo por el que he trabajado duro para conseguir que el ámbito conceptual en `www.social.engineer.org` incluya historias actualizadas y estudios de casos que puede emplear para mejorar sus habilidades.

En última instancia, todos estos ataques funcionaron porque la gente está diseñada para confiar en los demás, sentir compasión, empatía y el deseo de ayudar. Éstas son cualidades que no se deben perder, ya que debemos interactuar con el resto de seres humanos cada día. No obstante, al mismo tiempo, estas cualidades son las que explotan los ingenieros sociales maliciosos. Puede parecer que estoy defendiendo que nos convirtamos en criaturas endurecidas y carentes de sentimientos como un robot. Aunque eso le mantendría protegido, haría que la vida no tuviera sentido. Lo que defiendo es que sea consciente, que se forme y se prepare.

Resumen

La seguridad a través de la información es el mantra de este libro. Sólo cuando es consciente de los peligros que existen, sólo cuando sabe cómo piensan los delincuentes y sólo cuando está preparado para enfrentarse a ese mal, puede protegerse realmente. Con ese objetivo, el capítulo final de este libro explica cómo prevenir y mitigar los ataques de ingeniería social.

9. Prevención y mitigación

Los capítulos anteriores le enseñan todos los métodos y vías por las que los ingenieros sociales y los estafadores consiguen que sus objetivos revelen información valiosa.

También describen muchos de los principios psicológicos que utilizan los ingenieros sociales para influenciar y manipular a la gente.

Muchas veces, después de ofrecer un curso o impartir una conferencia sobre seguridad, la gente se muestra paranoica y temerosa y dice cosas como "parece que no hay posibilidad de protegerse. ¿Cómo puedo hacerlo?".

Ésa es una buena pregunta. Yo aconsejo tener un plan de recuperación de desastres y un plan de respuesta a incidentes porque hoy en día parece que no es una cuestión de "si" le van a atacar sino de "cuándo" lo harán. Puede tomar precauciones para, al menos, luchar por protegerse.

La mitigación no es tan sencilla como asegurar la protección del hardware. Con la seguridad defensiva tradicional puede gastar dinero en sistemas de detección de intrusos, programas antivirus y otras soluciones para mantener protegido el perímetro. Con la ingeniería social no existen sistemas de software que pueda emplear para proteger a sus empleados y a usted mismo.

En este capítulo, explico los seis pasos que les digo a mis clientes que pueden dar para prevenir y mitigar los intentos de ataque de ingeniería social:

- Aprender a identificar los ataques.
- Crear un programa personal de concienciación.
- Concienciar sobre el valor de la información que se busca.
- Mantener actualizado el software.
- Desarrollar guiones.
- Aprender de las auditorías de seguridad.

Estos seis puntos se reducen a crear una cultura de concienciación en seguridad. La concienciación no consiste en un programa de 40, 60 o 90 minutos todos los años. Consiste en crear una cultura o grupo de estándares con los que cada persona debe comprometerse a utilizar toda su vida. No se reduce a los trabajos o sitios Web considerados "importantes", sino al modo en que se afronta la seguridad como un todo.

Este capítulo explica los mencionados seis pasos y cómo crear una cultura de concienciación en seguridad es la mejor defensa contra los ingenieros sociales maliciosos.

Aprender a identificar los ataques

La primera fase de la prevención y mitigación es aprender sobre los ataques. No es necesario que profundice tanto en estos ataques como para saber crear archivos PDF maliciosos o a elaborar la estafa perfecta. Pero comprender qué sucede cuando abre un PDF malicioso y a qué señales prestar atención para determinar si alguien está tratando de engañarle puede ayudarle a protegerse. Necesita comprender las amenazas y cómo le afectan.

Aquí tiene un ejemplo: usted valora su casa y las cosas que hay dentro pero sobre todo a las personas que hay en la casa. No espera a sufrir el primer incendio para pararse a planear, prevenir y mitigar sus peligros. En lugar de eso, instala detectores de humo y planifica una ruta de huída en caso de incendio. Además, puede que instruya a sus hijos a "detenerse, tirarse y rodar" si se ven envueltos en un incendio. Les enseña a palpar la puerta para comprobar su temperatura y a mantenerse agachados para no respirar humo. Todos estos métodos son maneras de prevenir y prepararse para un incendio antes de sufrir uno y tener que lidiar con sus devastadoras consecuencias.

El mismo principio se aplica a la protección contra ataques de ingeniería social. No espere a que suceda el ataque para darse cuenta de lo devastador que puede ser. No piense que se lo digo por propio interés, pero aconsejo que se lleven a cabo auditorías de seguridad de manera regular para poner a prueba la habilidad de sus empleados de resistir estos ataques.

Enseñe a sus empleados cómo "detenerse tirase y rodar", en lo que se refiere a este tipo de ataques. ¿Cuáles son las últimas noticias sobre métodos de ataque a empresas? Conocerlas puede ser un buen método de defensa, igual que saber lo que un fuego puede provocar en su hogar. Aprenda los diferentes métodos que emplean los ingenieros sociales modernos y los ladrones de identidad. Puede encontrar un archivo de noticias y ejemplos de ingenieros sociales, estafadores, ladrones de identidad, etc. en `www.social-engineer.org/framework/Social_Engineering_In_The News`.

Otro buen paso es leer este libro. Contiene los métodos y principios que emplean los ingenieros sociales para manipular a sus objetivos. Este libro es más que una compilación de historias y ataques increíbles; ofrece un análisis del pensamiento y las tácticas utilizadas por los ingenieros sociales maliciosos.

Vea también los vídeos en el sitio `www.social-engineer.org` en el área de recursos (Resources), que muestran explotaciones en acción. El usuario medio no necesita verlos con la intención de entender cómo realizar estos ataques, sino para entender cómo realiza el ataque un profesional.

En esencia, cuanto más sepa sobre cómo suceden estos ataques, más sencillo le resultará identificarlos en la vida real. Ser consciente del lenguaje corporal, las expresiones y las frases empleadas en un intento de ataque hará que detecte enseguida cuándo alguien está empleando estos métodos.

No necesita pasar mucho tiempo aprendiendo sobre estos métodos. No obstante, dedicando unos minutos de vez en cuando a leer las noticias y las historias de `www.social-engineer.org` u otros sitios, puede comprobar los métodos que se emplean hoy en día contra las empresas. Cuando posea una buena base de conocimiento y haya realizado una auditoría, el siguiente paso, crear una cultura mentalizada con la seguridad, resultará sencillo de realizar.

Crear una cultura personal de concienciación

En julio de 2010 formé parte de un pequeño grupo de profesionales de la seguridad que organizó uno de los primeros concursos organizados de ingeniería social en Defcon 18. Algunas de las mentes más brillantes del planeta vienen a Las Vegas, Nevada, a hablar, enseñar y aprender.

Mi equipo y yo decidimos que sería una gran oportunidad para organizar un concurso que mostrara si el mundo corporativo de Estados Unidos era vulnerable a este vector de ataque (responder a un "concurso"). Organizamos el concurso haciendo que la gente interesada se registrara para formar parte en dos fases de ingeniería social: la recopilación de información y los ataques activos.

Para mantener el concurso dentro de la legalidad y la moralidad, no queríamos que hubiera víctimas, ni números de la Seguridad Social, ni tarjetas de crédito y no se reuniría información personal identificativa. Nuestra meta no era que despidieran a alguna de estas personas. Además, nuestra meta tampoco era avergonzar a ninguna empresa, por lo que decidimos que no se emplearían contraseña ni otros elementos de seguridad personal (información relacionada de las empresas). En lugar de esto, elaboramos una lista de unas 25 o 30 "banderas" que indicarían desde si la empresa tiene cafetería interna, quién se encarga de la recogida de residuos, qué navegadores utilizan y qué software emplean para abrir archivos PDF. Por último, elegimos empresas objetivo de todos los sectores de negocio: compañías de gas, empresas tecnológicas, fábricas, venta al por menor, etc.

A cada concursante se le asignaba una empresa en secreto sobre la que tenía dos semanas para llevar a cabo una recopilación pasiva de información. Esto significaba que a los concursantes no se les permitía contactar con la empresa, enviar correos electrónicos ni bajo ningún concepto tratar de sonsacar información con maniobras de ingeniería social. En su lugar, debían emplear la Web, Maltego y otras herramientas para reunir toda la información posible y preparar un informe profesional.

A partir de la información reunida, queríamos que los concursantes desarrollaran un par de vectores de ataque que creyeran que podrían funcionar en el mundo real. Después, los concursantes debían acudir a Defcon en Las Vegas, sentarse en un reservado insonorizado y realizar una llamada de 25 minutos al objetivo para implementar el vector de ataque y comprobar cuánta información podían obtener.

Podría dedicar 20 o 30 páginas a explicar lo que sucedió en el concurso y cuál fue el resultado, pero una de las cosas que descubrimos fue ésta: todos los concursantes obtuvieron tanta información de los objetivos que la empresa no habría superado una auditoría de seguridad. Independientemente del nivel de experiencia de los concursantes y su pretexto, todos tuvieron éxito logrando sus metas. Para ver un informe completo sobre el concurso y lo que ocurrió, visite `www.social-engineer.org/resources/sectf/Social-Engineer_CTF_Report.pdf`.

Vayamos a lo que es el tema de esta sección: concienciación en seguridad. Las empresas que se preocupan por la seguridad tienen programas con los que instruyen a sus empleados sobre cómo ser conscientes de los riesgos potenciales al teléfono, a través de Internet o en persona. Lo que descubrimos fue que la concienciación

en seguridad en esas empresas había fracasado. ¿Por qué? ¿Cómo era posible que estas empresas integrantes de la lista Fortune 500 que gastaban millones en seguridad, formación, educación y servicios diseñados para proteger a los empleados pudieran fracasar en la concienciación en seguridad?

Ésa es la idea que quiero expresar en el título de este capítulo: la concienciación no es personal para los empleados. A menudo, en mi práctica profesional, cuando hablo con empleados sobre sus sentimientos sobre un posible ataque, me responden con algo como "no son mis datos así que, ¿a mí qué me importa?". Esta actitud muestra que la concienciación no ha sido efectiva; no fue importante ni personal.

Revisando gran parte del material y los métodos disponibles sobre la concienciación en seguridad, lo que he descubierto es que es aburrida, tonta y no está pensada para que el participante interactúe o piense. Las breves presentaciones en DVD que abarcan gran cantidad de conceptos en un acercamiento forzado que acribilla al participante con pequeños datos no están diseñadas para llegar al fondo del asunto.

Lo que yo le animo a hacer, como empresa o como individuo, es crear un programa que atraiga, interactúe y profundice en la concienciación en seguridad. En lugar de explicarles a sus empleados por qué es buena idea tener contraseñas largas y complejas, demuéstreles lo sencillo que resulta descifrar una contraseña sencilla. Cuando me piden que ayude en la formación en concienciación para un cliente, a veces le pido a un empleado que se acerque a mi ordenador e introduzca una contraseña que crear que es segura. Esto lo hago antes de revelar ninguna información sobre contraseñas. Entonces, cuando empiezo mi presentación sobre esa sección, inicio un descifrador sobre esa contraseña. Normalmente, en un minuto o dos, se descifra la contraseña y revelo a todos los asistentes la contraseña secreta que se introdujo en mi ordenador. El efecto inmediato y drástico que tiene en cada persona es muy impactante. Pero después de varias demostraciones como ésta los empleados empiezan a comentar que ahora entienden lo importante que es tener una buena contraseña.

Cuando explico el tema de los adjuntos maliciosos en correos electrónicos, no tengo que enseñar a los empleados cómo crear un PDF malicioso pero sí les enseño el aspecto que tiene desde el ordenador del atacante y de la víctima cuando se abre el PDF malicioso. Esto ayuda a que comprendan que una simple falla puede conducir a la devastación.

Por supuesto, este método de enseñanza causa mucho miedo y, aunque ésa no es la meta, no es un mal efecto secundario, porque los empleados lo recuerdan mejor. Pero la meta es conseguir que piensen no sólo en lo que hacen en el trabajo y con los ordenadores de la oficina, sino con respecto a sus cuentas bancarias, ordenadores de casa y las amenazas que existen a nivel personal.

Quiero que cada persona que escucha una presentación de seguridad o lea este libro, revise cómo interactúa con Internet y hace cambios importantes para reutilizar contraseñas, almacenar contraseñas o información personal en localizaciones inseguras y dónde se conecta a Internet. No puedo decirle cuántas veces he visto a una persona sentada en medio de una cafetería aprovechando el *wifi* gratuito para comprobar una cuenta bancaria o hacer una compra *on-line*. En esas situaciones tengo que contenerme para no levantarme e ir a gritarle a esa persona lo rápidamente que su vida completa puede desmoronarse si la persona equivocada está en la misma red que ella.

También me gusta hacer pensar a la gente en el modo en que revelan información por Internet. Los estafadores y timadores utilizan muchas tácticas para robar a la gente mayor, a la gente con problemas económicos y al resto de gente. El teléfono todavía es una vía muy poderosa para hacer esto. Una forma de evitar muchos de los riesgos es conocer las políticas de los vendedores, bancos o proveedores sobre lo que pueden y no pueden preguntar por teléfono. Por ejemplo, muchos bancos señalan en sus políticas que no pueden pedir números de la Seguridad Social o números de cuenta. Saber esto puede evitar que caiga en esa estafa que puede hacerle perder los ahorros de toda su vida.

Llamar "programa" a la concienciación en seguridad indica que es algo en desarrollo. Un programa significa que organiza el tiempo para estar formándose continuamente. Después de obtener toda esta información, puede emplearla para desarrollar un programa que le ayude a protegerse.

Ser consciente del valor de la información que le están pidiendo

Volviendo al concurso de Defcon 18, en él aprendimos otra valiosa lección: cuando se percibe que la información tiene poco o ningún valor, entonces se hacen pocos esfuerzos por protegerla.

Ésta es una afirmación importante, pero se demuestra con la cantidad de objetivos que están dispuestos a revelar información. Debe ser consciente del valor de la información que posee y conocer las tácticas que pueden aplicarse para reducir a sus ojos el valor de esa información.

Antes de revelar información a alguien, determine si esa persona es digna de esa información. Los seres humanos tienen este deseo inherente de ayudar a quienes perciben que lo necesitan. Es una de las maneras más frecuentes que se emplean

para manipular a un objetivo para revelar información. Analizar a la persona con la que interactúa y determinar si merece esa información que pide puede ahorrarle el convertirse en una víctima.

Por ejemplo, en el concurso de Defcon un concursante desarrolló el pretexto de que era un cliente de una gran empresa de antivirus. Llamó con un problema importante. Su ordenador no se conectaba y creía que tenía que ver con la actividad del antivirus y quería que un técnico hiciera algo muy sencillo: entrar en un sitio Web.

Los ingenieros sociales maliciosos utilizan este vector de ataque muy a menudo. Llevando al objetivo hacia un sitio Web o unos archivos con código malicioso pueden acceder a su ordenador y su red. En el caso del concurso, el sitio Web no era malicioso, pero se demostró que si se hubiera realizado un ataque malintencionado, habría tenido éxito.

El primer intento fue diseñado por el concursante de esta forma: "No puedo entrar en mi sitio Web y creo que la razón es que su producto me está bloqueando. ¿Puede comprobarlo entrando en el sitio Web, para estar seguro de si es su software o no?".

El técnico respondió bien diciendo: "Señor, nuestro producto no le bloquea el acceso a ese sitio; no importa si yo puedo entrar o no". Declinó la petición.

El concursante no se dio por vencido; después de hablar por unos momentos, lo intentó de nuevo: "Ya sé que me ha dicho que su producto no puede bloquear mi sitio Web, pero funcionaba hasta que instalé el software, ¿puede comprobarlo por mí?".

De nuevo, rechazo la petición: "Señor, lo siento por las molestias pero nuestro producto no le bloquea el acceso al sitio Web y el hecho de que yo entre no le ayudará a solucionar el problema".

Parecía que la petición iba a ser rechazada definitivamente, pero el concursante intentó una última vía: "Señor, me quedaría más tranquilo si lo intentara un momento. Por favor, ¿puede ayudarme?".

Esta sencilla petición puso al técnico en una situación comprometida. Abrió su navegador y entró en el sitio Web. Había tomado la decisión correcta, había dado la respuesta adecuada, pero al final su deseo de que el "cliente" se "sintiera mejor" hizo que accediera a lo que le pedían. Esto podría haber conducido a la empresa a un gran riesgo si hubiera sido un ataque malintencionado.

El técnico sabía que esta información no era relevante para esa llamada en concreto. Al igual que él, debe analizar si la información que se le pide es relevante para la persona con la que interactúa.

Abordando este escenario desde el otro ángulo, ¿qué hubiera pasado si el concursante hubiera sido realmente un cliente y el técnico hubiera rechazado entrar en la Web? ¿Qué es lo peor que habría sucedido?

El cliente podría haberse molestado un poco por que se rechazara su petición pero no hubiera cambiado nada. El producto no era la causa de sus problemas. Un ingeniero social, a menudo, utiliza el encanto personal para iniciar una conversación sobre el tiempo, el trabajo, el producto, cualquier cosa, y lo utiliza para obtener la información que busca. Aquí es donde entra en juego una buena política de concienciación: instruir a sus empleados sobre las tácticas que se pueden emplear en su contra puede evitar que tomen decisiones equivocadas.

En una auditoría utilicé el pretexto de ser el ayudante de un director de finanzas. Los empleados de la centralita tenían miedo a perder sus trabajos si rechazaban las peticiones de un alto cargo. ¿Por qué? No tenían la formación adecuada para saber que rechazar esas peticiones no les haría perder sus trabajos. Al mismo tiempo, deben existir protocolos de actuación para que el empleado sepa cuándo una petición de información es apropiada.

El valor percibido de la información solicitada está íntimamente conectado con que una persona formada y educada sea consciente de que hasta los datos más insignificantes pueden conducir a una gran brecha. El empleado puede responder más adecuadamente si sabe que la persona al otro lado del teléfono no tiene por qué saber el nombre de la empresa de *catering*. Si es un empresario, debe ayudar a sus empleados a desarrollar respuestas para estas peticiones. En la mayoría de los casos un sencillo "lo siento, no poseo esa información; por favor, contacte con nuestro departamento de compras" o "lo siento, no estoy autorizado para revelar esa información pero puede enviar un correo electrónico a `info@company.com` para solicitar ayuda" puede anular la mayoría de intentos de ataque.

He mencionado anteriormente que crear una atmósfera que haga que la información parezca menos valiosa también es una táctica empleada por ingenieros sociales para conseguir que la gente se sienta cómoda revelando esta información "insignificante".

Empleando de nuevo el ejemplo del concurso, pedimos a un concursante que proporcionara cierta información identificativa. Su pretexto era una empresa que había sido contratada para realizar una auditoría interna y, cuando el objetivo quiso verificar quién era, pidió algo distinto. El concursante pretendió inclinarse hacia un compañero imaginario y dijo: "Jane, el caballero de Su-Empresa-Objetivo quiere el número de solicitud, ¿puedes hacerme el favor de cogerla de la mesa de Bill?".

Mientras "Jane" iba a buscar el número de solicitud, el concursante enredó al objetivo en una charla trivial. "¿Qué tiempo hace por Texas?" y "¿alguna vez has estado en el pub Charlie?" fueron evolucionando hacia "¿quién se encarga de la comida de la cafetería?" y "¿quieres ver una Web estupenda en la que estamos trabajando?".

Todo esto tenía lugar mientras "esperaba" el número de solicitud. Los ingenieros sociales emplean estas tácticas a diario. La desviación y el encanto son piezas clave de muchos pretextos. La información que se pide durante una charla es percibida

como insignificante por el momento de la conversación en que se pide. Si el ingeniero social hubiera hecho esa misma pregunta cuando estaba "verificando los resultados de su auditoría" se hubiera topado con una actitud muy distinta, pero como planteó la pregunta durante una conversación amistosa, recibió la información sin mayores problemas.

Se puede mitigar esta táctica de ataque reflexionando sobre el valor de la información que se plantea revelar independientemente del momento de la conversación en que se solicita. En el ejemplo anterior, el objetivo había evitado que lo embaucaran si hubiera esperado ese número de solicitud sin continuar la conversación.

Este punto es difícil de implementar porque los empleados, sobre todo los que trabajan de cara al cliente, deben tener la capacidad de proporcionar cierta información sin miedo a un ataque. Ser conciente del valor de la información no detiene el ataque por sí solo.

Mantener actualizado el software

En la mayoría de negocios, debe tener la capacidad de revelar información al público y a los clientes. Incluso en mi negocio debo proporcionar mi número de teléfono, direcciones de correo electrónico y direcciones Web. Debo poder enviar y recibir archivos PDF y poder hablar libremente por teléfono con mis clientes y proveedores.

No obstante, los puntos tratados hasta ahora indican que revelar esta información puede ser un peligro para el negocio y la privacidad. ¿Qué puede hacer para tener la libertad de revelar cierta información sin temores?

Manténgase actualizado. En nuestro concurso, más del 60 por 100 de las empresas contactadas todavía estaban utilizando Internet Explorer 6 y Adobe Acrobat 8. Estas estadísticas son asombrosas.

Sólo en esas dos aplicaciones existen docenas, sino cientos de vulnerabilidades. Saber que el objetivo utiliza esos dos programas los hace susceptibles a un enorme número de ataques que pueden ser tan maliciosos que ni los ID, los firewall ni los sistemas antivirus podrían neutralizarlos. No obstante, ¿sabe lo que sí los neutralizaría?

La respuesta es: las actualizaciones. Las versiones más actuales de software normalmente han cerrado sus brechas de seguridad, al menos la mayoría de ellas. Si un software tiene una trayectoria horrible, no lo utilice; cambie a algo menos vulnerable.

El problema que surge es que las empresas suelen ser muy lentas en lo que respecta a las actualizaciones. Internet Explorer 6 es muy antiguo, prácticamente está al final de su vida en Microsoft Support. Adobe 8 tiene docenas

de explotaciones disponibles al público. Esto es sólo una pequeña parte de la información que descubrimos en el concurso. La realidad es que tiene que ser capaz de facilitar información. Debe tener la libertad de comunicarse con los demás. Para hacerlo sin preocupaciones, debe asegurarse de que sus empleados utilicen software actualizado.

En las llamadas del concurso, si el empleado hubiera dicho que la empresa utilizaba Firefox, Chrome o algún otro navegador seguro, o FoxIt o el software más actual de Adobe, los concursantes habrían perdido las opciones. No estoy diciendo que esas aplicaciones no sufran ningún problema. Existen explotaciones para algunas versiones, pero es un software significativamente menos vulnerable. La posesión de esta información sigue siendo valiosa, pero si no hay explotaciones disponibles, la siguiente fase del ataque no puede lanzarse.

Mantener el software actualizado es un consejo que suele recibir muchas críticas, porque es el que más trabajo conlleva y el que se puede pasar por alto más a menudo. Cambiar las metodologías y las políticas internas que permiten la utilización de software anticuado puede ser complicado y causar todo tipo de cambios internos.

No obstante, si una empresa está comprometida con la seguridad y con crear la concienciación en seguridad personal, entonces comprometerse con estos cambios se convertirá en parte de la cultura del negocio.

Desarrollar guiones

Conviene mencionar otra actitud beneficiosa: desarrollar guiones. No tema; no quiero decir que los empleados tengan que decir X si la situación es igual a A más B. Estoy hablando de esquemas que ayuden al empleado a estar preparado para utilizar el pensamiento crítico cuando más lo necesita. Considere estos escenarios:

¿Cuál es la respuesta adecuada si llama alguien que dice trabajar para el director general y le pide su contraseña? ¿Cómo reaccionar si un tipo que no tiene cita pero tiene el aspecto y actúa como un vendedor solicita el acceso a cierta parte del edificio?

Los guiones pueden ayudar al empleado a determinar la respuesta adecuada en estas circunstancias y ayudar a que se sienta cómodo. Por ejemplo, un guión puede ser así:

Si llama alguien que dice ser de la oficina del gerente y pide que se le proporcione información interna, siga los siguientes pasos:

1. Pida el nombre y el número de identificación de empleado. No conteste ninguna pregunta hasta que posea esta información.

2. Después de obtener la información de identificación, pida el número identificativo de proyecto relacionado con el proyecto en el que esté trabajando y que requiera la información que está solicitando.
3. Si obtiene satisfactoriamente la información de los pasos 1 y 2, acceda. Si no, pida a la persona que solicite a su supervisor que envíe un correo electrónico solicitando la autorización y concluya la llamada.

Un guión sencillo como éste puede ayudar a los empleados a saber qué decir en circunstancias que pongan a prueba su concienciación en seguridad.

Aprender de las auditorías de seguridad

Si alguna vez ha sufrido la fractura de un miembro, sabrá que como parte de la recuperación el médico le mandará a rehabilitación. Durante ese proceso, puede ser objeto de pruebas dolorosas. Esas pruebas permiten a los médicos comprobar si sufre alguna debilidad que deba ser reforzada. Lo mismo se aplica a sus negocios, excepto que, en la auditoría, la prueba se realiza antes de que ocurra la brecha.

La siguiente sección responde algunas preguntas clave sobre las auditorías de seguridad y sobre cómo elegir al mejor auditor. Antes de profundizar en el asunto, debe saber qué es exactamente una auditoría.

Comprender lo que es una auditoría de seguridad

Básicamente, una auditoría de seguridad es donde un profesional de la seguridad es contratado para poner a prueba a la gente, las políticas y el perímetro físico de una empresa simulando los mismo ataques que emplearía un ingeniero social malicioso. Las dos diferencias principales entre el auditor y el ingeniero social malicioso son:

- Normalmente, el auditor seguirá unas directrices legales y morales.
- La meta del auditor de seguridad es siempre ayudar, no avergonzar, robar o dañar a sus clientes.
- Las auditorías profesionales tienen generalmente una limitación de alcance que no se imponen los atacantes reales.

El auditor profesional dedicará mucho tiempo a analizar y reunir información sobre el "objetivo" o cliente y empleará esa información para desarrollar vectores de ataque realistas. Mientras hace esto, el auditor siempre tiene en mente las metas establecidas para la auditoría. Ésta es una pieza fundamental del puzle, porque puede ser tentador ir por un camino que puede tener repercusiones muy negativas tanto para el auditor como para el objetivo. Las metas claramente definidas evitan que el auditor cometa ese tipo de error.

Establecer las metas de la auditoría

El auditor profesional debe comprometerse con una conducta ética y moral, a la vez que se mueve por la línea que le permite actuar como un verdadero ingeniero social malicioso. Esto implica tomar nota de las cosas que puede utilizar para acceder y explotar una brecha o debilidad en las defensas de la empresa, por muy rastrero que parezca.

Debe existir un equilibrio entre la búsqueda de fallas de seguridad y la preocupación por los empleados. A menudo, las empresas que son atacadas piensan que despedir al empleado que cayó en el ataque arregla el problema y tapa el "agujero". Lo que esos clientes no comprenden es que, después de una auditoría, esos empleados que sucumbieron al ataque probablemente son los más seguros del edificio.

El auditor profesional debe tomar precauciones para asegurar que los empleados no sean puestos en la línea de fuego. Personalmente, para mí es un punto clave explicar a las empresas que la auditoría no tiene que ver con los empleados y, siempre que puedo evitarlo, no doy nombres de los empleados que utilizo. En los casos en los que no puedo evitar mencionar esos nombres, centro el informe en los fallos de la empresa en su formación, sus políticas y sus defensas, que provocaron que el empleado fuera engañado.

Poner en riesgo el trabajo de un empleado nunca puede ser una opción para un auditor profesional. Cuando defino las metas de una auditoría señalo el nivel de intensidad, de 0 a 10, en estas áreas clave:

- Determinar si los empleados hacen clic en vínculos de correos electrónicos o abren archivos de gente que no conocen bien, provocando la situación comprometida.
- Determinar si un empleado entrará en un sitio Web e introducirá información personal o relacionada con la empresa.
- Determinar cuánta información puede obtenerse por teléfono o mediante visitas en persona a empleados en el trabajo o en otros lugares (como bares, gimnasios, guarderías, etc.).

- Determinar el nivel de seguridad en el perímetro de la oficina comprobando cierres, cámaras, sensores de movimiento y guardias de seguridad.
- Determinar la habilidad del ingeniero social para crear un USB o DVD malicioso que atraiga al empleado a utilizarlo en el ordenador del trabajo, comprometiendo a la empresa.

Por supuesto, se ponen a prueba otras áreas, pero lo que intento es determinar claramente las metas que tiene la empresa para la auditoría. Lo que descubro a menudo es que las empresas no saben lo que quieren. El trabajo del auditor es llevarles por ciertos caminos en la empresa para que determinen cuáles quieren poner a prueba.

Cuando se definen claramente estas metas, también debe incluir una lista de cosas que nunca deben hacerse en una auditoría.

Lo que debe y no debe incluirse en una auditoría

Existen muchas formas de poner a prueba las metas definidas para ver claramente si existe una falla en la empresa. Emplear todos los principios incluidos en este libro puede ayudar a definir un buen plan de ataque. Sin embargo, evite ciertos elementos cuando planifique el ataque. Cosas como:

- Atacar a la familia o amigos del objetivo.
- Colocar pruebas de delitos o infidelidades para desacreditar a un objetivo.
- Entrar por la fuerza en el hogar del objetivo.
- Emplear las pruebas de una aventura amorosa o una circunstancia embarazosa para chantajear a un objetivo.

Este tipo de cosas debe evitarse a toda costa porque no cumplen la meta y dejan al objetivo con la sensación de haber sido violentado. No obstante, surge la pregunta de qué hacer si en una auditoría aparecen evidencias de alguna de estas circunstancias. Cada auditor debe decidir personalmente cómo manejar estas situaciones, pero considere un par de ejemplos.

En una auditoría, el auditor descubrió que un empleado estaba utilizando la banda ancha de Internet de la empresa para descargar gigabytes de porno a discos externos. En lugar de poner en riesgo que despidieran al empleado, fue a hablar con él para decirle lo que había descubierto y para advertirle que lo dejara. El empleado se mostró muy avergonzado y molesto y pensó que de todas maneras el auditor

iba a denunciarlo. Decidió anticiparse a la situación y habló con los dueños de la empresa para decirles que el auditor estaba colocando pruebas falsas en su ordenador. Por supuesto, el auditor tenía registros y capturas de pantalla que probaban lo que había ocurrido en realidad y el empleado fue despedido de todos modos. Pero el auditor también fue reprendido por no informar sobre una incidencia para la que la empresa tenía una política muy estricta.

En otra situación, el auditor encontró evidencias de un hombre que descargaba pornografía infantil en su ordenador y después la distribuía a través de Internet. El auditor sabía que el empleado tenía mujer e hijos y que si lo denunciaba provocaría su divorcio, probablemente su ingreso en la cárcel y la ruina de su carrera y de su vida familiar.

La ley local establecía que la pornografía infantil es ilegal, además de moralmente vergonzosa y vil. El auditor denunció a aquel hombre a su empresa y a las autoridades, lo que le costó su carrera, su familia y su libertad.

Definir claramente una lista con las cosas que no debe hacer en sus auditorías le ayudará en el trabajo y evitará que cruce sus propios límites morales y legales. En una entrevista que tuve con Joe Navarro, uno de los más eminentes comunicadores no verbales del mundo, hizo una declaración sobre este asunto. Dijo que, a no ser que sea un agente de la ley, debe decidir qué líneas va a cruzar y cuáles no, antes de iniciar la actuación. Con esto en mente, ¿qué cosas deben incluirse en una auditoría?

- **Ataques de phishing:** Ataques dirigidos vía correo electrónico que permitan a la empresa comprobar si sus empleados son susceptibles a un ataque de este tipo.
- **Ataques en persona empleando el pretexto:** Se eligen pretextos muy precisos y controlados para desarrollar en persona o al teléfono para determinar si engañan al objetivo.
- **Ataques para picar el anzuelo:** Un ataque en persona en el que se accede al edificio del objetivo y se colocan llaves USB o DVD con archivos maliciosos.
- **Seguir la cola (o ir a remolque):** Un ataque en persona en el que el auditor se une a un grupo de empleados para acceder al edificio simplemente siguiéndolo.
- **Seguridad física (Red Team):** Un intento de lograr el acceso físico a una oficina para hacerse con objetos valiosos de la empresa.

Esta corta lista puede ayudar al auditor profesional a definir lo que debe y no debe ser incluido. Aun así, uno de los problemas más importantes de las empresas es elegir a un buen auditor, uno que pueda realizar estas tareas con eficacia.

Elegir al mejor auditor

Si se rompe un miembro y el daño es considerable y el médico le dice que sólo tiene un 50 por 100 de probabilidades de recuperarse, pero que consultar a un buen cirujano puede aumentar esas probabilidades, ¿no buscaría por todas partes un buen cirujano que arregle su problema? Y, cuando lo encuentre, ¿qué le preguntaría? ¿No le gustaría conocer su trabajo anterior? Querrá cierta prueba de sus conocimientos y su habilidad para realizar las tareas que aumenten sus opciones de recuperarse.

Seguirá un proceso parecido para encontrar al auditor adecuado. Aquí tiene algunos de los elementos fundamentales que debe averiguar cuando hable con un auditor:

- **Conocimientos:** ¿El equipo ha llevado a cabo alguna investigación, artículo, conferencia u otro material que demuestre que tiene conocimientos sobre ingeniería social? ¿Son conocidos en la comunidad por ser líderes en este campo? No debe confiar su auditoría a un equipo que emplea métodos anticuados y no esté al día de las últimas tácticas utilizadas.

  Es difícil determinar la profundidad del conocimiento de un equipo de auditores sin llevar a cabo cierta investigación. Puede ser buena idea pedirle al auditor cualquier tipo de artículo o información que haya escrito sobre estos temas. Asegúrese de que el equipo que contrate sea líder en el sector.

- **Experiencia:** A menudo, los clientes no quieren ser nombrados o mencionados. En mi caso, no quieren aparecer en un sitio Web o material de marketing porque les parece algo embarazoso o no quieren que eso les haga más vulnerables. Pero puede determinar la experiencia del auditor de otras maneras. Pregúntele sobre los métodos que ha empleado y cómo ha implementado soluciones en el pasado.

  Habitualmente, los auditores se resisten a revelar todos sus secretos en una primera reunión, pero pregúntele por un par de ataques que haya lanzado, lo que le ayudará a determinar sus niveles de habilidad.

- **Contrato:** Tener la auditoría perfectamente documentada, perfilada y con los límites establecidos, es importante cara al éxito final. A nivel personal, no me gusta trabajar con una tonelada de limitaciones porque la mayoría de los ingenieros sociales maliciosos no tienen limitaciones en absoluto. Pero al menos conviene acordar una pequeña lista de reglas escritas con lo que está permitido hacer y lo que no.

El auditor necesitará permiso para grabar llamadas telefónicas; grabar en vídeo el edificio y las interacciones; y especialmente si la auditoría implica seguridad física, el auditor necesitará un permiso firmado para llevarse cosas del lugar. El auditor no querrá terminar la auditoría y encontrarse con una orden de arresto o una demanda.

Además, designe una persona de contacto que tenga conocimiento de la auditoría y pueda responder por el auditor y su equipo. Si el auditor se encuentra en un problema legal necesitará un número al que llamar. A nadie le gusta estar registrando los contenedores por la noche, que aparezca la policía y acabar en la cárcel. Una persona de contacto proporciona un "salvoconducto" para salir de la cárcel y puede evitar muchas molestias a largo plazo.

- **Compenetración:** Aplique los principios de este libro para encontrar un buen auditor. Cuando hable con él por teléfono o en persona, ¿cómo le hace sentir? ¿Qué es lo que ve? ¿Le da la sensación de que es una persona profesional y que su verdadera meta es ayudarle?

  ¿El retrato que hace el equipo de sí mismo hace que quiera asociarse con él? Si es el encargado del proyecto que contrata al auditor, tiene una gran responsabilidad. Puede que el auditor no quiera reunirse con un equipo. Cuanta menos gente conozca su aspecto, mejor será a la hora de realizar auditorías físicas. En consecuencia, el equipo puede que solamente quiera reunirse con una o dos personas. Esto implica que debe asegurarse de que el auditor sea de gran calidad y que por lo tanto pueda realizar el trabajo requerido.

- **Tiempo:** Uno de los errores más frecuentes de las empresas a la hora de buscar auditor es no concederles el tiempo suficiente para hacer su trabajo. Piensan que hacer unas cuantas llamadas telefónicas y una visita al edificio puede hacerse todo en un día. Aunque esto puede que sea cierto, ¿qué sucede con la recopilación de información, la planificación y el reconocimiento del objetivo? Estas cosas llevan tiempo. El tiempo es importante pero también es un arma de doble filo: otórguele al auditor el tiempo suficiente para hacer su trabajo, pero no tanto que suponga un problema financiero. Administre, pero busque el equilibrio.

Éstos son sólo algunos de los puntos a tener en cuenta a la hora de elegir al auditor adecuado para su empresa.

El equipo de ingeniería social debe velar por su interés, mantener la profesionalidad y seguir las directrices.

Observaciones finales

El conocimiento no tiene valor alguno si no se lleva a la práctica.
Antón Chéjov

La información que proporciono en este libro no tiene un tono desenfadado. Mucha de esta información muestra serias vulnerabilidades en el modo en que la gente piensa y actúa. Cuando imparto clases de seguridad con mi mentor, Mati, siempre habla de un codificador de contenido llamado *shikata ga nai*, que en japonés quiere decir "no hay nada que hacer" o, traducido toscamente, "no hay esperanza".

Pensé en utilizar esta frase como epígrafe, pero consideré que la frase "no hay esperanza" es más fatalista de lo que me gusta resultar. En su lugar, creo que la reflexión sobre el conocimiento y la práctica encaja mejor con la temática del libro. He afirmado una y otra vez que perfeccionar las habilidades y la capacidad para detectar esas habilidades supone mucho más que mero conocimiento. Mostrarse temeroso ante las cosas que he mencionado en el libro conduce al enfado por todas las formas en que la gente puede ser atacada, lo que sólo nos puede conducir por un camino que provoca que cerremos nuestras mentes. En lugar de eso, sugiero afrontar esta información de un modo distinto: una mentalidad nueva que le anime a aprender y pensar y comprender los métodos que emplean los "chicos malos", para que pueda estar protegido ante sus ataques.

No estoy diciendo que haya que dejar el miedo completamente de lado. Es importante sentir cierta medida de miedo sano. Lo más beneficioso es proteger sus datos, su información personal y su identidad, pero al mismo tiempo comprender la mentalidad del hacker en combinación con la información de este libro.

Esta sección señala algunos puntos que espero que pueda extraer de este libro para emplearlos en su vida, especialmente si está al cargo de la seguridad de su empresa, sus clientes o si lee esto para su protección personal.

La ingeniería social no siempre es negativa

Espero haber demostrado que la ingeniería social no siempre es negativa. No siempre son los hackers o los estafadores quienes emplean estas tácticas. Médicos, terapeutas, trabajadores sociales, padres de familia, hijos, jefes, empleados, todo el mundo emplea tácticas de ingeniería social en cierto sentido. El arte de la persuasión se utiliza a menudo en situaciones del día a día.

A la hora de descubrir cómo se utilizan ciertas habilidades, es bueno aprender que la ingeniería social no siempre es inquietante, oscura y malvada. Cuando comprenda esas habilidades, practique hasta dominarlas; discernir cómo se emplean contra las personas resultará entonces mucho más sencillo.

Puede encontrar lugares para analizar estas técnicas que no tienen por qué estar en los rincones más oscuros del planeta. Puede leer libros sobre psicología, persuasión y ventas y observar cómo se utilizan estas técnicas en la vida real.

La importancia de recopilar y organizar la información

No puedo repetir las veces suficientes lo importante que es una recopilación de información de calidad. La calidad, profesionalidad y el éxito mismo de toda auditoría depende del nivel de recopilación de información que lleve a cabo. La Web es una fuente inagotable y abierta de información. Las empresas publican sus historiales financieros, los nombres y títulos de sus empleados, información de contacto, fotos de localizaciones físicas, políticas de seguridad, contratos, nombres de proveedores, archivos personales, etc. A nivel personal, los empleados y la gente en general publica fotos personales, direcciones, compras, alquileres, contratos, comidas favoritas, equipos deportivos, gustos musicales, etc.

Con esta cantidad de información en el bolsillo, un auditor puede elegir cuál quiere utilizar y qué tipo de ataque lanzar. Según avance la auditoría, la información reunida le dará al ingeniero social la habilidad para crear argumentos y pretextos que tengan el mayor efecto en el objetivo. Sin la recopilación de información, como hemos repetido a lo largo del libro, lo más probable es que la auditoría fracase.

Por ejemplo, si a un auditor profesional se le conceden tres semanas para realizar un trabajo, "debe" utilizar la mitad de ese tiempo para reunir información. No obstante, muchos auditores tienden a ponerse nerviosos y abordar a los objetivos con los mismos socorridos pretextos. No caiga en este hábito; pase mucho tiempo reuniendo información.

Casi tan importante como la recopilación de información es el modo en que la guarda y cataloga. Quizá puede hacerlo empleando uno de los métodos mencionados en el capítulo 2. Si aprende, no sólo a reunir eficientemente la información, sino a almacenarla correctamente, hará un uso más eficiente de ella. No vuelque datos en un documento enorme, catalogue la información, etiquételа y conseguirá que sea fácil de utilizar, sobre todo si debe realizar una acción al teléfono.

Recuerde que un ingeniero social sólo es tan bueno como la información que reúna. He visto fracasar muchas auditorías por culpa de una mala o escasa información. Por otro lado, he visto a personas que puede que no sean los mejores oradores o los más encantadores tener éxito en situaciones muy difíciles gracias a la información que manejaban.

La información es la clave de la ingeniería social y, si debe extraer una conclusión de este libro, que sea ésta.

Elija sus palabras cuidadosamente

Al igual que el epígrafe del inicio de este capítulo, este tema conduce a la idea de que la información no tiene valor a no ser que la ponga en práctica. Puede tener toda la información reunida, organizada y catalogada, pero debe utilizarla con eficiencia. El primer paso para ello es organizar las palabras que va a emplear.

He explicado las maniobras de obtención de información y la carga previa. Éstas son dos de las habilidades más valiosas y espero que las practique. Utilice anclajes, palabras clave, frases para cargar a su objetivo con emociones y pensamientos que hagan que siga su pauta. La carga previa es una técnica muy poderosa que no puede dominarse a corto plazo, pero la práctica le permitirá utilizarla. Lo mejor de la carga previa es que puede practicarla en casa, en el trabajo, con sus hijos, sus padres, sus clientes y en cualquier parte.

No piense que practicar esta técnica significa que deba conseguir en todo momento que la gente actúe contra su voluntad. La carga previa se emplea para motivar a la gente para que se abran a nuevas ideas o sugerencias. No es necesario emplearla con malas intenciones. Los niños lo hacen constantemente. Por ejemplo, su hija dice: "Papá, te quiero" y unos minutos después añade: "¿Puedo comprarme una muñeca nueva?".

Esto es un ejemplo de carga previa en la que se pone al objetivo en un estado mental de aceptación.

Cuando domine esta técnica, trabaje en sus maniobras de obtención de información. Recuerde que a nadie le gusta tener la sensación de estar siendo interrogado. Estas maniobras no deben imitar un interrogatorio policial; debe ser una conversación fluida y suave, empleada para reunir información sobre el objetivo o el asunto que desea.

Aprender los métodos y los procesos empleados para encontrar las preguntas a plantear en una conversación no sólo mejorará sus habilidades como auditor de seguridad, sino también como comunicador.

La gente disfruta cuando siente que los demás se interesan por su vida y su trabajo. Utilizar esta habilidad para bien mejorará su habilidad como ingeniero social.

Tengo una buena amiga que consigue que la gente le cuente cualquier cosa. Es increíble. Completos desconocidos dicen al final de la conversación: "No sé por qué te cuento estas cosas...". No está relacionada con el mundo de la seguridad, pero es un genio sonsacando información.

Dominar estas técnicas también mejorará su habilidad para planificar lo que va a decir. Le pondrán en el estado mental adecuado para buscar y reunir información de manera más inteligente y menos indiscreta.

Tenga un buen pretexto

Recuerde que un buen pretexto no es una mentira o una historieta. Debe convertirse y vivir su pretexto durante un tiempo. Cada parte de su ser (sus pensamientos, sus acciones, su discurso y su motivación) debe reflejar el pretexto que está desarrollando. Si puede lograr esto su pretexto resultará creíble para el objetivo.

Otro punto a recordar es que el pretexto se emplea todos los días, no sólo en ingeniería social. Imagine esta situación: acaba de discutir con su pareja. Ahora está en el trabajo y no quiere que nadie sepa que las cosas en casa no van bien, así que cuando algún compañero le pregunta: "Eh, Jim, ¿cómo va todo?", responde: "genial, gracias".

Esto es justo lo contrario a la verdad, pero ¿cómo consigue que resulte creíble? Sonríe y proyecta confianza con su postura corporal. Dependiendo de su deseo de privacidad, puede que incluso desarrolle una historia para demostrar lo bien que van las cosas.

Ésta es sólo una situación posible, pero la gente utiliza el pretexto todo el tiempo. Siempre que intenta disfrazar la realidad ante la gente está utilizando un pretexto. Por supuesto, mucha gente no consigue hacerlo bien y es descubierta fácilmente. Detectar estas situaciones le otorgará una buena base de análisis del pretexto.

Analizar estos escenarios le ayudará a identificar las áreas en las que debe mejorar en sus pretextos y a dominar esta técnica tan útil.

Practique leyendo expresiones

Creo que podría hablar durante semanas de las microexpresiones. El tema me fascina y me intriga pensar que la gente tiene mecanismos inherentes para demostrar sus más profundos sentimientos sin tener control sobre ellos. El modo en que las emociones provocan que ciertos músculos se contraigan y muestren cierta expresión durante una fracción de segundo es un aspecto increíble de la creación. Pero aprender a detectarlas, leerlas y emplear esas mismas expresiones para manipular a los demás es algo que realmente me deja estupefacto.

Practique recreando las microexpresiones explicadas en el capítulo 5. Al hacerlo, observe las emociones que le provocan esas expresiones. Practicarlas le ayudará a detectarlas en los demás.

Cuando practique no se centre sólo en leer las microexpresiones en los demás, sino en controlar sus propias microexpresiones y en evitar que alguien pueda leer las suyas. Recuerde que leerlas en otros es una buena habilidad, pero tener el control de sus propias microexpresiones, lenguaje corporal y tonos vocales es mucho más interesante. Esta habilidad puede mejorar su práctica profesional y sus relaciones

personales. Cuando domine estas técnicas, empezará a darse cuenta de cómo puede utilizar uno de los conceptos principales del capítulo 5, el desbordamiento de búfer humano. La mente humana funciona de un modo parecido a un software, pero a un nivel superior. Pero puede ser distorsionado, examinado y sobrepasado como un software. Relea esa sección para asegurarse de comprender perfectamente los principios explicados.

Manipulación e influencia

La manipulación y la influencia son dos aspectos de las interacciones sociales que tienen efectos espectaculares y poderosos en la gente con la que interactúa. Por este motivo, utilice la información explicada en el capítulo 6 con mucho cuidado. Aprender a persuadir y manipular a la gente puede marcar literalmente la diferencia entre el éxito y el fracaso. Cada día la gente intenta manipular y persuadir a otros para realizar ciertas acciones. Algunas de estas acciones son malas y pueden costar dinero, libertad personal e identidades.

Utilice esas situaciones como herramientas de aprendizaje. Analice los métodos de los comerciales, psicólogos, orientadores, profesores y compañeros de trabajo que intentan manipularlo. Elija los puntos de los que considere que puede aprender e intégrelos en su arsenal.

Recuerde que la persuasión no siempre es negativa: no siempre significa hacer que alguien realice una acción que no desea. La persuasión puede tener efectos muy positivos y, muchas veces, la persuasión positiva es mucho más difícil de llevar a cabo. Si domina estas habilidades y las emplea para ayudar a la gente a protegerse, estará más preparado para identificarlas cuando alguien las emplee en un sentido negativo.

Manténgase alerta a las tácticas maliciosas

Ser consciente de las tácticas que los atacantes utilizan a buen seguro evitará que sea víctima de ellas. Los auditores profesionales pueden emplear esas tácticas para educar a sus clientes sobre las cosas en que fijarse para detectar un posible ataque. Manténgase alerta para distinguir casos en los que se emplean esas tácticas.

Por ejemplo, una táctica que emplean los "chicos malos" es golpear en tiempos problemáticos. Cuando los aviones chocaron con las Torres Gemelas, los terremotos sacudieron Haití y el tsunami arrasó en Asia, la devastación entre la población y sus vidas, psique y emociones era incalculable. Durante este tiempo de vulnerabilidad y debilidad es cuando los chicos malos golpean.

Permítame ilustrarlo del siguiente modo: en cierta ocasión leí un artículo que hablaba sobre los métodos de caza de los leones. Explicaba que un león, cuando quiere confundir y separar al grupo de presas para elegir a una víctima, ruge hacia el suelo; no hacia las presas o hacia el cielo, sino hacia el suelo. ¿Por qué? Porque el descomunal e intimidatorio rugido reverbera en el suelo y rodea a las presas. Les invade la confusión al no saber en qué dirección viene el león. Algunas se dispersarán hacia la derecha, otras hacia la izquierda, pero dejarán a los miembros jóvenes, viejos y enfermos al descubierto.

Este ejemplo no está muy alejado del modo en que los ingenieros sociales maliciosos operan. "Rugen" de tal modo que causan confusión. Emplean sitios Web que ayudan a encontrar a los seres queridos desaparecidos después de un desastre natural o afirman haber perdido a familiares ellos mismos. Cuando las emociones de los "objetivos" están tan implicadas que no pueden pensar con claridad, es cuando el ataque tiene lugar.

Los inexpertos y los inmaduros (tecnológicamente hablando) son los primeros en caer víctimas revelando información hasta que el atacante consigue la suficiente para elaborar un perfil. Ese perfil ayuda a lanzar ataques posteriores y éstos cada vez son más despiadados y crueles.

Esté atento a estos casos y mantendrá a sus clientes protegidos de ser víctima de ellos. También utilice estas situaciones como aprendizaje, analice los métodos empleados y compruebe si funcionaron o fracasaron. De este modo, mejorará su habilidad para estar más alerta a amenazas potenciales.

La desgraciada diferencia entre un león y un ingeniero social (aparte de las obvias) es que un ingeniero social no lanza un rugido audible. No está ahí fuera gritando: "¡Quiero una presa, todos a correr!". En lugar de eso, sus ataques ladinos y sutiles engañan a miles de personas cada año.

Utilice su miedo

Si este capítulo ha hecho que sienta algo de miedo, sólo puedo decir: "Bien". Lo necesita. Porque el miedo sano puede salvar su vida o, al menos en este caso, su identidad y su negocio.

Utilice ese miedo para motivar el cambio. No se enfade ni se disguste. Tome la decisión de formarse a usted, a su familia y a sus empresas sobre cómo observar, detectar y defenderse de los ataques. Tome la decisión de no permitir que se pirateen sus identidades y sus empresas y haga algo al respecto.

Este libro se resume en la idea de "seguridad a través de la formación". El pirateo humano es una forma de arte. La ingeniería social es una mezcla y combinación de ciencias, arte y habilidad. Cuando se combinan en las cantidades adecuadas el resultado es *shikata ga nai*.

Las empresas pierden millones de euros cada año por causa de las brechas de seguridad, con una gran mayoría de ellas producto de ataques de ingeniería social. No obstante, cuando ofrecemos a nuestros clientes incluir una auditoría de ingeniería social en nuestras pruebas de seguridad, suelen declinar la oferta.

¿Por qué?

Las empresas tienden a temer los cambios. En incontables ocasiones, en mi experiencia profesional, he escuchado a empresarios inteligentes y exitosos decir cosas como: "No necesitamos una auditoría. Nuestra gente no caería en esos trucos". Después, durante las pruebas de seguridad realizamos alguna llamada autorizada para obtener información y cuando la presentamos en el informe se sorprenden de lo sencillo que nos resulta conseguirla.

En distintos niveles empresariales la concienciación en seguridad no suele variar mucho. Cuando hablamos con las empresas sobre los programas de concienciación que impartimos, muchas nos dicen que no realizan formación para los departamentos de soporte técnico o la centralita de llamadas. Sin embargo, ésos son los departamentos que más a menudo caen en ataques de ingeniería social.

Esto apunta al núcleo del problema del que hablo. La seguridad a través de la formación no puede ser simplemente una frase pegadiza; debe convertirse en una declaración de objetivos. Hasta que las empresas y las personas que forman esas empresas no se tomen la seguridad en serio y a nivel personal, el problema no se arreglará completamente. Mientras tanto, aquéllos que se lo toman lo suficientemente en serio como para leer este libro y tener el deseo de observar los rincones oscuros de la sociedad, pueden mejorar sus habilidades lo suficiente como para mantener a sus familias y empresas un poco más protegidas.

Cuando "ruja el león" sea el líder al frente de la manada dirigiendo el éxodo. Sea un ejemplo sobre lo que hay que hacer y cómo defenderse de estos ataques.

Con el tiempo y la dedicación suficientes, cualquier persona puede ser víctima de un ataque. Esas palabras son duras pero ciertas. Eso no significa que no haya esperanza; significa que su trabajo es conseguir que los ataques sean tan complicados y costosos que los hackers decidan que no merece la pena y vayan a buscar a una víctima más asequible. Lo sé; esto suena desalmado. Me encantaría que todo el mundo leyera este libro y llevara a cabo cambios radicales, entonces las empresas estarían realmente protegidas. Pero ése no es el mundo en el que vivimos.

Esa afirmación, por tanto, conlleva una pregunta importante. Si realmente no hay esperanza, ¿cómo pueden las empresas, la gente y las familias protegerse de las vulnerabilidades? Hasta que las empresas empiecen a ser conscientes de su vulnerabilidad ante los ataques, los individuos deberán formarse a sí mismos sobre los métodos de ataque y mantenerse alerta, así como difundir el mensaje a los demás. Sólo entonces tendremos la esperanza de mantenernos un paso por delante de los ataques.

Resumen

Al finalizar este libro, espero que le haya abierto los ojos al mundo de la ingeniería social. Deseo que siga ayudándole a tener en cuenta el potencial de los ataques maliciosos. También me gustaría que haya contribuido a construir o mantener un miedo sano al desastre potencial.

También espero que este libro le ayude a proteger sus negocios, su familia, sus hijos, sus inversiones y su vida. Espero que la información que contiene le haya demostrado que no es imposible mantenerse completamente protegido.

Mati Aharoni, mi mentor, dice en una de sus clases que la razón por la que los chicos malos suelen ganar es porque ponen más dedicación, tiempo y motivación. No permita que nada se interponga en el camino de la seguridad. No obstante, tampoco permita que el miedo de los chicos malos le impida disfrutar de la vida.

Espero que al aplicar los principios de este libro mejore su habilidad para comunicarse con más eficiencia con quienes le rodean. Utilizarlos en distintos aspectos de su vida, no sólo en el campo de la seguridad, puede convertirse en un ejercicio que cambie su vida. Verdaderamente, la ingeniería social es una forma de arte. Disfrute.

Índice alfabético

A

B

C

D

E

F

G

H

I

U

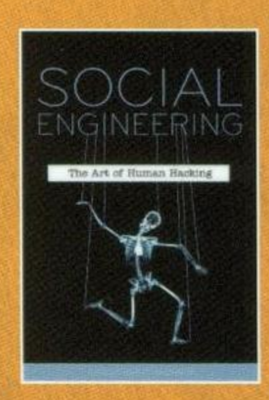
V

W

Páginas Web

Del original:

Social Engineering
The Art of Human Hacking
WILEY



Chris le mostrará cuándo surgen las situaciones de peligro y cuáles son las estrategias de ingeniería social utilizadas por los intrusos hoy en día. Su libro le ayudará a adquirir un mayor entendimiento para reconocer este tipo de ataques".

Kevin Mitnick, escritor, orador y consultor.

"Chris Hadnagy ha redactado el libro más importante hasta ahora escrito sobre ingeniería social. Ampliamente documentado, lleno de aplicaciones prácticas, este estupendo libro ofrece soluciones a los problemas y peligros que acechan su negocio y a usted mismo. Realmente innovador".

Kevin Hogan , autor de *El arte de la persuasión: cómo lograr que alguien diga "sí" en 8 minutos o menos.*



INGENIERÍA SOCIAL

EL ARTE DEL HACKING PERSONAL

La mayoría de ataques informáticos tienen un componente desafiante, doloroso, confuso. Sin embargo un ingeniero social experimentado es un arma letal contra la que resulta imposible defenderse. Su singularidad y arriesgadas soluciones pueden solventar las vulnerabilidades técnicas más imprevistas.

Chris Hadnagy ha escrito el libro definitivo sobre ingeniería social y conseguido unánimes elogios. Meticulosamente documentado y repleto de aplicaciones prácticas, esta obra define, explica y analiza cada principio para ilustrarlo con historias reales, dando soluciones a los problemas y peligros del mundo virtual.

Descubra los secretos de manipuladores y estafadores experimentados. No importa lo sofisticados que sean sus procedimientos y sistemas de seguridad, su punto más vulnerable es y será el sólido entramado social.
Lea con atención estas páginas y descubrirá con seguridad quién es su enemigo.

Recorra el oscuro mundo de la ingeniería social a través de los siguientes temas:

- Los principios psicológicos empleados por los ingenieros sociales y cómo utilizarlos.
- Los secretos de la persuasión.
- Cómo los delincuentes sacan partido de cámaras, dispositivos GPS y la identificación de llamadas.
- Cómo encontrar la información en Internet.
- Los argumentos de los ingenieros sociales.

